Applying Jennings theory and the $\mathcal{M}$-series to modular isomorphism problems

by

Jan Nyquist Roksvold

Thesis for the degree of

Master in Mathematics

(Master of Science)

Department of Mathematics
Faculty of Mathematics and Natural Sciences
University of Oslo

May 2011

Acknowledgments

Thanks to my advisors Inger Christin Borge and Arne Bernhard Sletsjøe, for enthusiasm and good advice throughout, and for always keeping an open door. To the latter also for excellent courses on commutative algebra and representation theory.
To Benjamin Klopsch and Donald Passman, for trying to help me prove that the $\mathcal{M}$-series is an N-series.
To Robin Bjørnetun Jacobsen, for proofreading and clever suggestions.

Most of all, I would like to thank my parents, for their exceptional kindness and support all these years.

Contents

Chapter 1

Introduction

For G a group and R a commutative ring with unity, let $R[G]$ be the set of all formal sums $\sum_{g\in G} \alpha_g g$, with $\alpha_g \in R$ and $\alpha_g = 0$ for all but a finite number of gs.

With addition defined componentwise

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (a_g + \beta_g) g,$$

$R[G]$ is a free R-module with basis G. Furthermore, the group multiplication offers a natural way of multiplying elements; we define

$$\Big(\sum_{x\in G} \alpha_x x\Big)\Big(\sum_{y\in G} \beta_y y\Big) = \sum_{z\in G} \lambda_z z, \text{ where } \lambda_z = \sum_{xy=z} \alpha_x \beta_y$$

The multiplication is associative because multiplication in G is, and gives $R[G]$ the structure of an R-algebra. This construction is commonly referred to as the group algebra or **group ring** of G over R.

Although an attractive object of study in itself, the group ring has historically been considered a tool for studying (finite) groups, for example through representations and characters. This is particularly effective when G is finite and $R = \mathbb{K}$ is a field, as the theory of finite dimensional $\mathbb{K}$-algebras is considerably more advanced than that of finite groups ([25]).

Starting out with a problem in group theory, typically one concerning a particular group G, one may construct the group ring over some suitable ring R; applying either general results from ring theory, or particular results about group rings, one hopes to discover something about $R[G]$ that can be translated back into purely group-theoretical results about G.

The effectiveness of this method relies upon knowledge about which parts of the structure of G that are conserved by $R[G]$, and which parts that are not. We would like to know how much is lost in translation.

We say that a property, or feature (e.g. the isomorphism class of a subgroup) of G is *determined* by $R[G]$ if whenever H is another group and $R[G] \cong R[H]$ as R-algebras, then H also possesses the property/feature. In other words, a feature of G is said to be determined if it can be induced from the structure of $R[G]$ as an R-algebra.

Whenever $R[G] \ncong R[H]$ the (necessarily non-isomorphic) groups G and H are said to *split* over R.

The "ideal" situation would be if it was true that for all rings R and groups G, the group itself – that is, the isomorphism class of G – was determined by $R[G]$. Unfortunately, this is easily dismissed: if $\mathbb{C}$ is the set of complex numbers and G is finite and abelian, then $\mathbb{C}[G]$ is a semisimple commutative algebra and from [18, Corollary 2.4.2] we have

$$\mathbb{C}[G] \cong \mathbb{C}^{|G|}$$

as a $\mathbb{C}$-algebra.[1] In other words, we have

$$\mathbb{C}[G] \cong \mathbb{C}[H]$$

for every abelian group H with $|H| = |G|$.

The correct question, then, appears to be: given certain conditions on G and R, is it true that a certain feature of G is determined by $R[G]$? Questions of this type are commonly referred to as *isomorphism problems*, and whenever the property in question is the strongest one possible, namely the isomorphism class of G itself, we shall somewhat informally refer to the isomorphism question as being *strong*.

Assume G is finite.[2] Typical isomorphism questions could for example be:

(i) Is the order of G determined by $\mathbb{K}[G]$ for every field $\mathbb{K}$?

(ii) Does $\mathbb{Z}[G]$ determine the centre $\mathcal{Z}(G)$ of G?

(iii) Is G itself determined by $\mathbb{Z}[G]$?

(iv) Is an abelian p-group determined by its group algebra over a field of characteristic p?

[1] These are of course always isomorphic as $\mathbb{C}$-*vector spaces*, as they have equal dimension.

[2] There certainly are isomorphism problems for infinite groups as well, but these are beyond the scope of this thesis. For an uncountable group G, the modular isomorphism problem has, to the best of my knowledge, not even been solved for the case when G is abelian and $\mathbb{K} = \mathbb{F}_p$. We will suffice to say that when G is infinite, very little is known ([25]).

(v) If $\mathbb{F}_p$ is the field of p elements and G is a p-group, does $\mathbb{F}_p[G]$ determine G?

The answer to (i) is clearly yes, as the order of G is equal to the dimension of the finite dimensional algebra $\mathbb{K}[G]$.

Number (ii) was positively decided by Berman (see [33, Corollary 3.2]). So if $\mathbb{Z}[G] \cong \mathbb{Z}[H]$, then $\mathcal{Z}(G) \cong \mathcal{Z}(H)$.

Question (iii) is the classical *integral isomorphism problem*, initially posed by Graham Higman in [11] (1940). In his survey [33] published in 1985, Sandling reports that:

> "Although this problem has been addressed for over 40 years, it is yet to be resolved. Because of its difficulty, effort expended on it has the potential for uncovering significant facts about group rings or methods for their analysis."

The problem was actually not to be solved for another 16 years, until a counterexample was found by Martin Hertweck and published in [10] (2001).

Question (iv) was positively decided by Deskins in [5] (1956). A second proof can be found in [4], and a third, but incorrect, proof is found in [26]. We offer a fourth proof in Chapter 5.

Question (v) is the *modular isomorphism problem* (MIP), which forms the backdrop for this thesis. A stronger variant is

> **(MIP)** If G is a finite p-group and $\mathbb{K}$ is a field of characteristic p, does $\mathbb{K}[G]$ determine G?

Many (in fact, most) of the invariants so far found have only been established for the "light" version $\mathbb{K} = \mathbb{F}_p$. On the other hand, this is all that is needed for many purposes, for example that of establishing whether a couple of finite p-groups G and H are isomorphic or not; if the strongest version of the MIP was positively decided, it would still not be any point in looking for isomorphisms between $\mathbb{K}[G]$ and $\mathbb{K}[H]$ for other fields of characteristic p than $\mathbb{F}_p$, as this would just be unnecessarily complicated.

It is also important to be aware that $\mathbb{F}_p[G]$ determines $\mathbb{K}[G]$ for every group G and every field $\mathbb{K}$ of characteristic p. For if H is a group with

$$\mathbb{F}_p[G] \cong \mathbb{F}_p[H]$$

then

$$\mathbb{K}[G] \cong \mathbb{K} \otimes_{\mathbb{F}_p} (\mathbb{F}_p[G]) \cong \mathbb{K} \otimes_{\mathbb{F}_p} (\mathbb{F}_p[H]) \cong \mathbb{K}[H].$$

In general, we shall refer to the group ring over a field of prime characteristic as the *modular* group ring. If the group is a p-group, the

modular group ring is, unless otherwise stated, assumed to be over a field of characteristic p.

Research on the MIP may well be said to have gotten off on the wrong foot. The first written appearance seems to be the above mentioned article by Jennings from 1956, where he after having positively decided question (iv) above, claims that the theorem

> "... is not in general true for p-groups over a field of characteristic p. The dihedral group of order 8 and the quaternion group have isomorphic group algebras over $GF(2)$."

His conclusion *might* be correct, but – as was first pointed out by Coleman in [4] (1964) – the counterexample is not. We shall demonstrate in Section 5.4 that these two groups do in fact have non-isomorphic group rings, not only over $\mathbb{F}_2$, but over $\mathbb{F}_{2^n}$ for every odd number n.

Today, more than half a century after research on the MIP begun in earnest, it remains as the only strong isomorphism problem still open.

Despite Hertweck's counterexample to the strong integral isomorphism problem, it is true that for an arbitrary finite group G the integral group ring preserves the structure of G better than does $\mathbb{K}[G]$ for $\mathbb{K}$ a field. Naively, this is perhaps comparable to the fact that the more complex instrumental background music one adds, the harder it is to discern the vocal. The more advanced field-structure offers more opportunities than the integers for an isomorphism to arise between the group rings of non-isomorphic groups. In fact, a simple argument found in [26, p. 664] shows that $\mathbb{Z}[G]$ determines $\mathbb{K}[G]$ for every field $\mathbb{K}$.

For specific classes of groups however, certain fields have proven to be well suited as coefficients. That fields of characteristic p are indeed the "correct" ones for finite p-groups can be seen from the following result by Passman:

Theorem. *[23] There exists a set of at least $p^{2n^2(n-17)/27}$ non-isomorphic groups of order p^n that have isomorphic group rings over all fields of characteristic different from p.*

Although fields of characteristic p present the last glimmer of hope to positively confirm a strong isomorphism problem, there certainly are drawbacks to having the characteristic dividing the order of G. For one, we lose the whole of character theory (no inner product); in addition, as we shall see in Chapter 2, the modular group ring of a finite p-group fails to be semisimple, which can not only be seen as a disadvantage in itself – it also renders much of representation theory ineffective.

A significant advantage when the characteristic of $\mathbb{K}$ equals p, however, is that the otherwise mysterious[3] series of dimension subgroups all of a sudden turn into an accessible and valuable tool. The series of dimension subgroups of a modular group ring is equal to the so-called Brauer-Jennings-Zassenhaus series (or just $\mathcal{M}$-series), which has the desirable quality of being defined solely in terms of G, and hence, crucially, independent from the group ring.

This groundbreaking result was first[4] proved by S. A. Jennings in [15] (1941). Although never mentioning it explicitly, this paper has had an enormous impact on the MIP. The tools provided by Jennings in the article, most significant of which the *Jennings basis* and the *Jennings formula*, to a great extent compensate for the above mentioned losses.

Computations involving the dimension subgroups have been particularly useful for splitting groups in order to verify the MIP for "small" p-groups. The current status of this verification process is that all p-groups of order $\leq p^5$ for p odd, and all groups of order 2^n for $n \leq 8$, have been shown to split over $\mathbb{F}_p$.[5] The latter result was found using computers.

An important motivation for looking at "small" p-groups, is the hope of discovering a counterexample. As Hertweck says in [13]:

> "We have the feeling that the majority opinion on (MIP) is that there should be counterexamples, and that such will be found if just the sheer computer power needed to handle the calculations will be available. Let us recapitulate: theoretical results – so far known – impose only weak obstructions, and the complexity and number of p-groups increases dramatically with their order, so we won't find invariants general enough to split all groups.[...] Perhaps it is time to examine further groups of order p^6".

The contents of this thesis

In this thesis we shall focus mainly on certain descending sequences of subgroups, and their interplay with filtrations of the so-called augmentation ideal. The results, as well as the general direction taken, are motivated by the modular isomorphism problem. In particular, we investigate problems

[3] For free groups, the integral dimension subgroups are equal to the lower central series ([22, p. *ix*]). For arbitrary groups, however, the situation is much more complicated, and little use has been made of the integral dimension subgroups in connection to integral isomorphism problems ([33, p. 271]).

[4] Jennings only proves this for the case $\mathbb{K} = \mathbb{F}_p$. The full result can be found in [26], where it is attributed to Michel Lazard ([19], 1963).

[5] See [32].

related to the MIP using the Brauer-Jennings-Zassenhaus series (from now on, just $\mathcal{M}$-series).

We also attempt to give a direct proof that the $\mathcal{M}$-series is a so-called N_p-series, the achievement of which would constitute a new[6] proof that for a finite p-group over a field of characteristic p, the series of dimension subgroups is equal to the $\mathcal{M}$-series. Although a certain progress is made, the attempt is ultimately unsuccesful.

In **Chapter 2** we introduce the objects of study, crucially the augmentation ideal and series of subgroups (amongst them the N- and N_p-series). We also introduce an alternative basis for the augmentation ideal, one which is used repeatedly in Chapter 3. The main results are that the augmentation ideal of the modular group ring of a finite p-group is nilpotent, and that it is equal to the Jacobson radical[7]. Both of these results are of course well known.

As we shall only concern ourselves with group rings over fields, we completely ignore the possibility of using other rings as coefficients.

In **Chapter 3** we present Jennings's results concerning the modular group ring of a finite p-group. This requires the introduction of concepts such as filtrations and derived series of subgroups, and we give a brief treatment of these topics in advance. The main results are: the existence of a Jennings basis, the Jennings formula, and that the dimension subgroups constitute a minimal N_p-series.

In **Chapter 4** we loosen the restrictions on G – which can now be an arbitrary group. We begin by introducing the $\mathcal{M}$-series, and proceed to establish certain basic facts about it, for example that each $\mathcal{M}_i$ is a characteristic subgroup. Defining a suitable function, we obtain a non-recursive expression for the $\mathcal{M}$-series of an abelian group, thereby correcting a mistake in [26]. Towards the end, we attempt – and fail – to give a direct proof that the $\mathcal{M}$-series is an N_p-series

In **Chapter 5** we apply the results of chapters 3 and 4 to "isomorphism type" problems. We show that for $p > 2$, a certain class of p-groups, the so-called extraspecial ones, split over fields of characteristic p. We also extend a result by Passman which says that D_8 and the quaternions split over $\mathbb{F}_2$, by showing that these groups split over $\mathbb{F}_{2^n}$ for every odd number n. Using the newly found non-recursive expression from Chapter 4, we give a new proof that finite abelian p-groups split. Finally, we demonstrate how computations with the $\mathcal{M}$-series may be used to split "small" groups by splitting two non-

[6]The original proof of this was, as already mentioned, given in [15]. Other proofs are found in [27, Theorem 1.9], [26, Theorem 1.20] and [12, Theorem 8.2.7].

[7]See Appendix A.

abelian p-groups of order p^6.

In short, chapters 2 and 3 set the stage, while original contributions are found in sections 4.2 and 4.3, and in Chapter 5.

Chapter 2

Preliminaries

In this chapter we recall two of the well-known particularities of the modular group ring of a finite p-group: that the soon to be defined augmentation ideal is nilpotent, and that it is equal to the Jacobson radical[1].

As finite p-groups have a rich supply of normal subgroups, it is natural – and has proven fruitful – to study their modular group rings through sequences of such groups. This is the approach taken in this thesis as well, and in Section 2.2 we define, and establish some basic facts about, those sequences we shall encounter.

2.1 The augmentation ideal

Let G be a group and $\mathbb{K}$ a field. Then $\mathbb{K}[G]$ is a $\mathbb{K}$-algebra with basis G. The group ring $\mathbb{K}[G]$ is commutative if and only if G is abelian, and finite dimensional if and only if G is finite.

The **augmentation function** $\tau : \mathbb{K}[G] \to \mathbb{K}$ is given by

$$\tau\Big(\sum_{g\in G} \alpha_g g\Big) = \sum_{g\in G} \alpha_g.$$

This is a $\mathbb{K}$-algebra homomorphism, and so its kernel is a two-sided ideal of $\mathbb{K}[G]$.

Definition. *Let* $\Delta(\mathbb{K}[G]) = \{\sum_{g\in G} \alpha_g g : \sum_{g\in G} \alpha_g = 0\}$. *We call* $\Delta(\mathbb{K}[G])$ *the* ***augmentation ideal*** *of* $\mathbb{K}[G]$.

Whenever clear from the context, we omit referring to the specific group ring and simply write Δ in place of $\Delta(\mathbb{K}[G])$.

[1] See Appendix A.

Theorem 2.1. *The set of all* $(g-1)$ *with* $g \in G \setminus \{1\}$ *forms a basis for* Δ.

Proof. First observe that $(g-1) \in \Delta$ for all $g \in G$. The set of all $(g-1)$ with $g \neq 1$ is linearly independent because G is (by definition). It remains to show that the set span Δ; but if $\sum_{g\in G} \alpha_g g \in \Delta$, then $\sum_{g\in G} \alpha_g 1 = 0$ and

$$\sum_{g\in G} \alpha_g g = \sum_{g\in G} \alpha_g g - \sum_{g\in G} \alpha_g 1 = \sum_{g\in G} \alpha_g (g-1). \qquad \square$$

An element x of a ring R is said to be **nilpotent** if there is an $n \in \mathbb{N}$ such that $x^n = 0$. A **nil** (left, right, or two-sided) ideal is an ideal all of whose elements are nilpotent.

From now on, and throughout the rest of the thesis, we shall by ideal always mean a two-sided ideal. If I and J are ideals, we define their product IJ to be the set of all finite sums

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n, \text{ where } x_i \in I \text{ and } y_i \in J.$$

The product of two ideals is itself an ideal. We define $I^0 = \mathbb{K}[G]$.

We say that an ideal I is **nilpotent** if there is an $n \in \mathbb{N}$ such that

$$I^n = \{0\}.$$

Note that the multiplication of ideals is associative, which makes the expression I^n unambiguous. That I is nilpotent is equivalent to there existing an $n \in \mathbb{N}$ such that

$$a_1a_2 \cdots a_n = 0 \text{ for all } a_1, a_2, \ldots a_n \in I.$$

By definition, every nilpotent ideal is a nil ideal. The opposite however, is not true in general. In fact, many results in ring theory establish conditions under which a nil ideal is rendered nilpotent. One such result is:

Proposition 2.2. *If* G *is finite, then every nil ideal of* $\mathbb{K}[G]$ *is nilpotent.*

Proof. Because finite dimensional unital[2] algebras over fields are Artinian as rings (see [9, p. 19]), the result follows immediately from [9, Corollary 1.3.1], which says that in an Artinian ring every nil ideal is nilpotent. $\square$

Let $g \in G$. As 1 commutes with every element of $\mathbb{K}[G]$, we may apply the binomial formula in order to compute $(g-1)^n$. In particular, when $\mathrm{char}(\mathbb{K}) = p$ we have

$$(g-1)^p = \sum_{i=0}^{p} (-1)^i \binom{p}{i} g^{p-i} = g^p - 1,$$

[2] An algebra with a multiplicative identity element.

since $p \mid \binom{p}{i}$ for $1 \leq i \leq p-1$.

If in addition G is a finite p-group, then

$$(g-1)^{|G|} = g^{|G|} - 1 = 1 - 1 = 0, \text{ for all } g \in G. \tag{2.1}$$

In combination with Theorem 2.1, this shows that $\Delta(\mathbb{K}[G])$ has a basis of nilpotent elements. Since finite sums of nilpotent elements are nilpotent, we infer from Proposition 2.2 that $\Delta(\mathbb{K}[G])$ is a nilpotent ideal whenever G is a finite p-group and $\mathrm{char}(\mathbb{K}) = p$.

A partial converse: that if $\Delta(\mathbb{K}[G])$ is nilpotent then G is a finite p-group and $\mathrm{char}(\mathbb{K}) \neq 0$, was given by Gerald Loosey in [21]. For a proof of the complete result stated as Theorem 2.3 below, we refer to either [26, Lemma 3.1.6] or [27, Theorem 6.1.2].

Theorem 2.3. *The augmentation ideal $\Delta(\mathbb{K}[G])$ is nilpotent if and only if G is a finite p-group and $\mathbb{K}$ is a field of characteristic p.*

We refer to [9, Lemma 1.2.2] for a proof of

Lemma 2.4. *For any ring R, every nil ideal is contained in the Jacobson radical $\mathcal{J}R$ of R.*

The next result implies that the modular group ring of a finite p-group fails quite thoroughly to be semisimple[3].

Theorem 2.5. *If G is a finite p-group and $\mathrm{char}(\mathbb{K}) = p$, then*

$$\Delta(\mathbb{K}[G]) = \mathcal{J}\mathbb{K}[G].$$

Proof. Since Δ is nilpotent, we have $\Delta \subseteq \mathcal{J}\mathbb{K}[G]$ by Lemma 2.4. From Theorem 2.1 we see that Δ has codimension 1, and hence is a maximal ideal. We conclude that $\Delta(\mathbb{K}[G]) = \mathcal{J}\mathbb{K}[G]$. □

This also implies that the augmentation ideal of the modular group ring of a finite p-group is determined by the group ring *as a $\mathbb{K}$-algebra*; a fact which is crucial when tackling modular isomorphism problems, and one which shall be used repeatedly throughout this thesis.

Corollary 2.6. *If G is a finite p-group and $\mathrm{char}(\mathbb{K}) = p$, then $\mathbb{K}[G]$ determines $\Delta(\mathbb{K}[G])$.*

[3]Consult Appendix A for a definition of the term "semisimple".

In general, one would have to know the values of τ for a basis of $\mathbb{K}[G]$ in order to know $\Delta(\mathbb{K}[G])$.

Theorems 2.3 and 2.5 are deep results both of which stem from the seemingly innocuous equation (2.1). In fact, being such an immediate consequence of the definition of a field of characteristic p and of a finite p-group, this equation might be said to capture the very essence of the modular group ring. It certainly looms in the background of everything that we do in Chapter 3.

From these remarks one might expect Theorem 2.5 to be unique to the modular group ring of a finite p-group. And indeed, under the assumption that G is finite the converse of Theorem 2.5, namely that if $\mathcal{J}\mathbb{K}[G] = \Delta(\mathbb{K}[G])$ then G is a p-group and $\mathrm{char}(\mathbb{K}) = p$, follows immediately from Theorem 2.3 and the fact that in Artinian rings the Jacobson radical is nilpotent ([9, Lemma 1.3.1]). Without the assumption that G is finite, we may still conclude that $\mathbb{K}$ is a field of characteristic p and that G is a p-group with certain "finite-like" properties[4].

As our further study of the group ring will be in terms of descending sequences of subgroups, it is time for a short interlude in group theory.

2.2 Descending series

Let G be a group. We shall define a **series** $\{G_i\}$ to be a descending sequence of subgroups of G such that

$$G = G_1 \geqslant G_2 \geqslant \cdots .$$

Note that we require the first subgroup of the sequence to be G itself.

The series $\{G_i\}$ is said to be **1-stable** if there is a $d \in \mathbb{N}$ such that $G_{d+1} = \{1\}$. The least such d is the **length** of $\{G_i\}$.

A **finite** series is a series $\{G_i\}$ consisting of a finite number of subgroups and which terminates with $\{1\}$; in other words such that

$$G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_d > G_{d+1} = \{1\}$$

is all of $\{G_i\}$. According to these definitions a finite series is 1-stable, and if a 1-stable series $\{G_i\}$ of length d is not finite then $G_i = \{1\}$ for all $i > d$.

We briefly introduce the series we shall encounter. Most of the terminology that follows is in accordance with standard one found in e.g. [8]. A notable difference being that the chief and normal series are most commonly *defined* to be finite. Dropping the finiteness condition better suits our aims, and will make for a more fluent exposition.

[4] See [26, p. 416].

Definition. *A **normal** series is a series of subgroups that are normal in G.*

To each normal series we associate a sequence of factor groups G_i/G_{i+1}, $i \geq 1$.

Definition. *A **chief** series is a normal series such that G_{i+1} is either equivalent to – or a maximal normal subgroup of – G_i. In other words, a normal series all of whose factor groups are either trivial or simple.*

Central to group theory in general, and this thesis in particular, is studying the "difference" between xy and yx for elements $x, y \in G$. We define

$$[x, y] = x^{-1}y^{-1}xy,$$

and refer to this as the **commutator** of x and y.

If H and K are subgroups of G, let

$$[H, K] = \langle [h, k] : h \in H, k \in K \rangle.$$

Note that $[h, k] = [k, h]^{-1}$ implies $[H, K] = [K, H]$. The **commutator subgroup** $[G, G]$ of G has the property that if N is a normal subgroup of G, then

$$G/N \text{ is abelian if and only if } [G, G] \leqslant N.$$

Definition. *A series $\{G_i\}$ is said to be **central** if*

$$[G_{i-1}, G] \leqslant G_i \text{ for each } i > 1.$$

Proposition 2.7. *Every central series is normal.*

Proof. Let $\{G_i\}$ be a central series. If $g_i \in G_i$ and $g \in G$, then $g^{-1}g_i g = g_i[g_i, g]$ which is contained in G_i because $[g_i, g] \in G_{i+1}$. □

The **lower central series** $\{\gamma_i\}$ given by

$$\gamma_1 = G, \text{ and } \gamma_i = [\gamma_{i-1}, G] \text{ for } i > 1,$$

has the property that if $\{G_i\}$ is any central series, then $\gamma_i \leqslant G_i$ for all $i \geq 1$. In later chapters, we shall write $\gamma_i(H)$ whenever we feel the need to emphasize that we are dealing with the lower central series of a specific group H. The group H is said to be **nilpotent** whenever $\{\gamma_i(H)\}$ is 1-stable; in that case, the length d of $\{\gamma_i(H)\}$ is the **nilpotency class** of H, and H is said to be a class d group.

The series we introduce next are slightly more specialized, and important to the study of groups through their group rings.

Definition. *An* **N-*series*** *is a series* $\{G_i\}$ *with the additional property that*

$$[G_m, G_n] \leqslant G_{m+n} \text{ for all } m, n \geq 1.$$

This property is sometimes referred to as **strong centrality**. It follows directly from the definition that every N-series is central, and hence normal.

Definition. *Let* p *be a prime. We say that the series* $\{G_i\}$ *is* **p-*restricted*** *if*

$$x \in G_i \text{ implies } x^p \in G_{ip}.$$

Definition. *An* $\mathbf{N_p}$**-*series*** *is a* p*-restricted* N*-series.*

Let $\mathbf{C_n}$ denote the cyclic group of order n. The following definition is needed to accentuate the properties of an N_p-series.

Definition. *An* ***elementary abelian*** *group is a finite abelian group all of whose (nontrivial) elements have order* p *(for some prime* p*). In other words, a group of order* p^n *is elementary abelian if and only if it is isomorphic to* $\underbrace{C_p \times C_p \times \cdots \times C_p}_{n \text{ factors}}$.

Proposition 2.8. *Let* $\{G_i\}$ *be an* N_p*-series. Then for all* $1 \leq i < j \leq 2i$*, the factor group* G_i/G_j *is elementary abelian.*

Proof. The factor group is abelian because $[G_i, G_i] \leqslant G_{2i} \leqslant G_j$. Furthermore, for all $g \in G_i$ we have $g^p \in G_{ip} \leqslant G_{2i} \leqslant G_j$. □

2.3 An alternative basis

The single result of this section provides an alternative basis for $\Delta(\mathbb{K}[G])$. In Chapter 3, where G is assumed to be a finite p-group, this basis will be used to create a connection between any given N_p-series and Δ. In particular, it will serve as an excellent platform for the construction of *Jennings bases*, which shall be our main concern in Section 3.2.

The result can also be found, in a slightly less general form, as Lemma 3.4.3 in [26].

Theorem 2.9. *Let* $\mathbb{K}$ *be a field, and let* $G = H_1 > H_2 > \cdots > H_{n+1} = \{1\}$ *be a finite chief series satisfying* $|H_i/H_{i+1}| = p$*. Pick* $x_i \in H_i \setminus H_{i+1}$*. For each set* $\{a_1, a_2, \ldots, a_n\}$ *with* $0 \leq a_i < p$ *let*

$$\eta(a_1, a_2, ..., a_n) = (x_1 - 1)^{a_1}(x_2 - 1)^{a_2} \ldots (x_n - 1)^{a_n}.$$

(i) The set of all $\eta(0,...,0,a_j,...,a_n)$s forms a basis for $\mathbb{K}[H_j]$ as a $\mathbb{K}$-vector space.

(ii) This same set with $\eta(0,...,0)=1$ excluded, forms a basis for $\Delta(\mathbb{K}[H_j])$.

Proof. We shall prove (i) by reversed induction on j, and thus start by looking at the case $j=n$. Since there are (certainly no more than) $\dim_{\mathbb{K}}\mathbb{K}[H_n]=p$ elements of the form $(x_n-1)^{a_n}$ with $0\leq a_n<p$, it suffices to show that these span $\mathbb{K}[H_n]$.

So let $\alpha\in\mathbb{K}[H_n]$. Then

$$\alpha=\alpha_0+\alpha_1x_n+\alpha_2x_n^2+\cdots+\alpha_{p-1}x_n^{p-1},$$

for some $\alpha_s\in\mathbb{K}$. Since $x_n^s=(x_n-1+1)^s=\sum_{i=0}^s\binom{s}{i}(x_n-1)^i$, we have

$$\alpha=\sum_{s=0}^{p-1}\alpha_s\Big(\sum_{i=0}^{s}\binom{s}{i}(x_n-1)^i\Big),$$

which settles the case $j=n$.

Now assume the statement holds for $j+1\leq n$. Since the number of $\eta(0,...,0,a_j,...,a_n)$s are (at most) p^{n-j+1}, which is equal to $\dim_{\mathbb{K}}(\mathbb{K}[H_j])$, and since these are all contained in $\mathbb{K}[H_j]$, it will suffice to show that they span $\mathbb{K}[H_j]$. Observe that

$$H_j/H_{j+1}=\langle x_jH_{j+1}\rangle.$$

Let $\alpha=\alpha_1g_1+\alpha_2g_2+...+\alpha_kg_k\in\mathbb{K}[H_j]$. Assume that $g_i\in x_j^{l(i)}H_{j+1}$; then $g_i=x_j^{l(i)}h_i$ for some $h_i\in H_{j+1}$, and

$$\alpha=\alpha_1x_j^{l(1)}h_1+\alpha_2x_j^{l(2)}h_2+...+\alpha_kx_j^{l(k)}h_k.$$

Since the h_is can be expressed as a $\mathbb{K}$-linear term of $\eta(0,...,0,a_{j+1},...,a_n)$s by the induction hypothesis, and because

$$x_j^{l(i)}=((x_j-1)+1)^{l(i)}=\sum_{s=0}^{l(i)}\binom{l(i)}{s}(x_j-1)^s,$$

we are done.

For (ii), we observe that each $\eta(0,...,0,a_j,...,a_n)$ with not all a_is equal to zero is contained in $\Delta(\mathbb{K}[H_j])$. There are $|H_j|-1$ such ηs, and as these are linearly independent and because $1\notin\Delta(\mathbb{K}[H_j])$, they must span $\Delta(\mathbb{K}[H_j])$. □

We shall at times be needing the set $\{x_1,x_2,\ldots,x_n\}$ of x_is chosen from each of the subgroups H_i, and we shall refer to these x_is as the **representatives** of $\{H_i\}$.

Chapter 3

Jennings theory

Throughout this chapter, let G be a finite p-group and $\mathbb{K}$ a field of characteristic p. We recall from Theorem 2.3 that the augmentation ideal $\Delta(\mathbb{K}[G])$ is then nilpotent.

The purpose of this chapter is to present the results that originated in Jennings's paper [15]. In addition, we show that under the above fixed conditions, the series of dimension subgroups constitute *the* minimal N_p-series. Our exposition covers the same topics as [26, pp. 84-91], and all results and major proofs can – in some form or other – be found there as well. We do however present the material quite differently, beginning with the already introduced *representatives*, which will be put to work in Section 3.2.

In short, we offer no original contributions in this chapter, but simply organize and present the material occasionally referred to as *Jennings theory*.

3.1 Derived series and induced filtrations

Definition. *A **filtration** is a sequence $\{E_i\}$ of ideals such that*

$$\Delta(\mathbb{K}[G]) = E_1 \supseteq E_2 \supseteq \dots,$$

and

$$E_m E_n \subseteq E_{m+n}.$$

An important example is obtained by setting

$$E_i = \Delta^i.$$

This is a sequence of ideals (by Section 2.1), and it is certainly descending. That $\Delta^m \Delta^n = \Delta^{m+n}$ follows from the associativity of the multiplication

of ideals. Observe that $E_rE_s \subseteq E_{r+s}$ implies $\Delta^i = (E_1)^i \subseteq E_i$ for every filtration $\{E_i\}$.

For a filtration $\{E_i\}$, let

$$G_i = G \cap \{1 + E_i\}.$$

This is a subgroup according to the one-step subgroup test, for if $g, h \in G_i$ then

$$gh^{-1} - 1 = ((g-1) - (h-1))h^{-1} \in E_i$$

implies $gh^{-1} \in G_i$.

As $G_1 = \{g \in G : g - 1 \in \Delta\} = G$, it is clear that $\{G_i\}$ forms a series. We say that the series $\{G_i\}$ is **derived** from $\{E_i\}$.

Theorem 3.1. *Let $\{E_i\}$ be a filtration of Δ. The series $\{G_i\}$ obtained by setting $G_i = G \cap \{1 + E_i\}$ is an N_p-series.*

Proof. If $g_m \in G_m$ and $g_n \in G_n$, then

$$[g_m, g_n] - 1 = g_m^{-1}g_n^{-1}g_mg_n - 1 = g_m^{-1}g_n^{-1}(g_mg_n - g_ng_m),$$

which is contained in E_{m+n} because

$$g_mg_n - g_ng_m = (g_m - 1)(g_n - 1) - (g_n - 1)(g_m - 1) \in E_{m+n}.$$

We conclude that

$$[G_m, G_n] \leqslant G_{m+n}.$$

Also, if $g \in G_i$ then $(g-1)^p \in E_i^p \subseteq E_{ip}$. As $(g-1)^p = g^p - 1$ in characteristic p, we have $g^p \in G_{ip}$. □

An observation we shall use later on, is that the above proof did not use the fact that G is a finite p-group – and that the result therefore holds for any group.

We also note that the derived series $\{G_i\}$ is clearly 1-stable whenever $\{E_i\}$ at some point stabilizes at $\{0\}$. We shall soon see that the converse is true as well.

Definition. *Let $\{\mathcal{D}_i\}$ be the series derived from the powers of Δ, i.e.*

$$\mathcal{D}_i = G \cap \{1 + \Delta^i\}.$$

*These are the **dimension subgroups** of G. As Δ is nilpotent, the series of dimension subgroups is 1-stable.*

It is also possible to go the opposite direction: from a 1-stable N_p-series, we may construct a filtration of Δ. Our main tool in doing this is the function $\nu : G \to \mathbb{N} \cup \{\infty\}$ given by

$$\nu(g) = \begin{cases} d & \text{if } g \in G_d \smallsetminus G_{d+1} \\ \infty & \text{if } g = 1. \end{cases}$$

We shall say that $\nu(g)$ is the **height** of g.

In order to simplify notation, we immediately extend the height function ν to a certain subset of Δ, namely elements of the form

$$(g_1 - 1)(g_2 - 1) \cdots (g_k - 1),$$

by letting

$$w\big((g_1 - 1)(g_2 - 1) \cdots (g_k - 1)\big) = \sum_{i=1}^{k} \nu(g_i).$$

We shall call this the **weight** of $(g_1 - 1)(g_2 - 1) \cdots (g_k - 1)$.

Theorem 3.2. *Suppose $\{G_i\}$ is a 1-stable N_p-series and let E_i be the $\mathbb{K}$-linear span of all elements $(g_1 - 1)(g_2 - 1) \cdots (g_k - 1)$ with $g_j \in G$ and $\sum_{j=1}^{k} v(g_j) \geq i$. Then $\{E_i\}$ is a filtration of Δ.*

Proof. We infer from Theorem 2.1 both that $E_1 = \Delta$, and that each E_i is an ideal – as it is clearly closed under left and right multiplication with 1 and elements of the form $(g - 1)$. The sequence $\{E_i\}$ is clearly descending.

If π_m and π_n are generators of E_m and E_n, respectively, then

$$w(\pi_m \pi_n) = w(\pi_m) + w(\pi_n) \geq m + n,$$

which shows that $E_m E_n \subseteq E_{m+n}$. □

We shall refer to the above as the filtration **induced** by $\{G_i\}$; and to each of the $(g_1 - 1)(g_2 - 1) \cdots (g_k - 1)$ as a **generator** for E_i.

Theorem 3.3. *Let $\{G_i\}$ be a 1-stable N_p-series. If $\{E_i\}$ is the filtration induced by $\{G_i\}$, then $\{E_i\}$ at some point stabilizes at zero.*

Proof. Assume $G_d \neq G_{d+1} = 1$. Let n be a natural number, and let $\pi = (g_1 - 1)(g_2 - 1) \cdots (g_k - 1)$ be one of the generators for E_{nd}. Then

$$nd \leq \nu(g_1) + \cdots + \nu(g_k).$$

On the other hand, $\nu(g) \leq d$ for all $g \in G$, so

$$\nu(g_1) + \cdots + \nu(g_k) \leq kd.$$

Together this implies $nd \leq kd$ and $n \leq k$. As

$$\pi = (g_1 - 1)(g_2 - 1) \dots (g_k - 1) \in \Delta^k$$

it follows that $\pi \in \Delta^n \supseteq \Delta^k$, and since π was an arbitrary generator we conclude that $E_{nd} \subseteq \Delta^n$.

Since $\mathrm{char}(\mathbb{K}) = p$ and G is a finite p-group, there is an $N \in \mathbb{N}$ such that $\Delta^N = \{0\}$. By the above argument, $E_{Nd} \subseteq \Delta^N = \{0\}$. □

3.2 The Jennings basis

Throughout this section we assume that $|G| = p^n$, that $\{G_i\}$ is a 1-stable N_p-series, and that $\{E_i\}$ is the filtration induced by $\{G_i\}$.

By eliminating multiples of subgroups appearing more than once in $\{G_i\}$ we obtain a series $\{G'_i\}$ *without repetitions*, such that

$$G = G_1 > G'_2 > \cdots > G'_{r+1} = 1 \text{ (for some } r),$$

in which each element of $\{G_i\}$ occurs exactly once.

Inserting subgroups where possible, we may next refine $\{G'_i\}$ to a (finite) chief series

$$G = H_1 > H_2 > \cdots H_n > H_{n+1} = \{1\},$$

with each of the factor groups H_i/H_{i+1} simple. As the only simple finite p-groups are cyclic of order p, it is clear that $\{H_i\}$ satisfies the hypothesis of Theorem 2.9, and thus provides us with representatives

$$x_1, x_2, \dots, x_n$$

with which we construct a basis $\mathcal{B}$ of Δ.

An important observation is that each of the subgroups occuring in $\{G_i\}$ occurs (exactly once) in $\{H_i\}$. The opposite however, is not necessarily true.

In contrast to the treatment given in [26], we extract the following as a separate lemma. The only reason for doing this is to make the proof of Theorem 3.5 more palatable.

Lemma 3.4. *Each generator* $\pi = (g_1 - 1)(g_2 - 1) \dots (g_k - 1)$ *of* E_i *can be expressed as a* $\mathbb{K}$*-linear sum of elements of the form*

$$(x_{y(1)} - 1)(x_{y(2)} - 1) \dots (x_{y(k)} - 1) \quad \textit{with } \nu(x_{y(j)}) = \nu(g_j),$$

modulo E_{i+1}.

Proof. We start by singling out one of the factors $(g_j - 1)$, such that

$$\pi = \alpha(g_j - 1)\beta.$$

As $\{H_i\}$ is a refinement of $\{G_i\}$, we know that for some r,

$$G_{\nu(g_j)} = H_r > H_{r+1} > \cdots > H_{n+1} = 1.$$

From Theorem 2.9 then, we have that $(g_j - 1)$ is a $\mathbb{K}$-linear sum of elements of the form $(x_r - 1)^{a_r}(x_{r+1} - 1)^{a_{r+1}} \dots (x_n - 1)^{a_n}$. As $\nu(x_s) \geq \nu(g_j)$ for all $r \leq s \leq n$, we see that any such element consisting of more than one factor, or whose single factor has height greater than $\nu(g_j)$, is contained in $E_{\nu(g_j)+1}$. Therefore,

$$(g_j - 1) = \sum_{\nu(x_s)=\nu(g_j)} c_s(x_s - 1) + \gamma, \text{ where } \gamma \in E_{\nu(g_j)+1},$$

and

$$\pi = \sum_{\nu(x_s)=\nu(g_j)} c_s\alpha(x_s - 1)\beta + \alpha\gamma\beta, \text{ with } \alpha\gamma\beta \in E_{i+1}.$$

Repeating the argument for the remaining factors of π, we get the result. □

Theorem 3.5. *The set $\{\eta \in \mathcal{B} : w(\eta) = i\}$ forms a basis for E_i/E_{i+1} as a $\mathbb{K}$-vector space. We call this the* ***Jennings basis*** *of E_i/E_{i+1}.*

Proof. Since the ηs are linearly independent, and since every η with $w(\eta) = i$ is contained in E_i by definition, it will suffice to show that each generator of E_i is expressable as a $\mathbb{K}$-linear sum of ηs with weight i, modulo E_{i+1}. We shall prove this by strong induction on the number k of factors of the generator.

First, let π be a generator with only one factor. Then, by Lemma 3.4, we may assume $\pi = (x - 1)$ for some representative x with $\nu(x) \geq i$. Consequently, we have $\pi = (x - 1) + E_{i+1}$ or $\pi = 0 + E_{i+1}$, depending on whether $\nu(x) = i$ or $\nu(x) > i$. Either way, π is a $\mathbb{K}$-linear sum of ηs (one η, actually) with weight i, modulo E_{i+1}.

Now let $k > 1$, and let π be a generator for E_i containing k factors. Assume that the statement of the theorem holds for all generators containing fewer than k factors. By Lemma 3.4, we may assume that

$$\pi = (x_{y(1)} - 1)(x_{y(2)} - 1) \cdots (x_{y(k)} - 1).$$

We claim that we are actually free to assume that the factors of π are in their "natural" order, such that

$$\pi = (x_1 - 1)^{b_1}(x_2 - 1)^{b_2} \cdots (x_n - 1)^{b_n}, \text{ with } b_1 + b_2 + \cdots + b_n = k.$$

Assume for now that the claim is true. If each $b_j < p$ then π is itself an η, and thus π is equal to this η or 0 modulo E_{i+1}, depending on whether $w(\pi) = i$ or $w(\pi) > i$, respectively. On the other hand, if $b_j \geq p$ for some j then $(x_j - 1)^p = (x_j^p - 1)$ occurs as a factor in π. As $\{G\}$ is p-restricted, we know that $\nu(x_j^p) \geq p\nu(x_j)$, which means that π is equal to a product of less than k factors but with weight $\geq i$; in other words: another generator for E_i, but one which contains fewer than k factors. The result then follows from the induction hypothesis.

We return to prove our claim. Let $(x_u - 1)$ and $(x_v - 1)$ be two adjacent factors of π, such that

$$\pi = \alpha(x_u - 1)(x_v - 1)\beta.$$

Assume that $\nu(x_u) = r$ and $\nu(x_v) = s$, and consider the identity

$$(x_u - 1)(x_v - 1) = (x_v - 1)(x_u - 1) + ([x_u, x_v] - 1) + (x_v x_u - 1)([x_u, x_v] - 1).$$

Because $\nu([x_u, x_v]) \geq r + s$ by the definition of an N-series, we have

$$w\big((x_v x_u - 1)([x_u, x_v] - 1)\big) \geq \max\{r + 2s, 2r + s\},$$

which in turn implies

$$w\big(\alpha(x_v x_u - 1)([x_u, x_u] - 1)\beta\big) > w(\pi) = i,$$

such that

$$\alpha(x_v x_u - 1)([x_u, x_v] - 1)\beta \in E_{i+1}.$$

Consequently,

$$\pi = \alpha(x_v - 1)(x_u - 1)\beta + \alpha([x_u, x_v] - 1)\beta + E_{i+1}.$$

The term $\alpha([x_u, x_v] - 1)\beta$ is a product of $k - 1$ factors but has weight $\geq i$; by the induction hypothesis then, it can be expressed as a $\mathbb{K}$-linear sum of ηs with weight i, modulo E_{i+1}. It therefore suffices to show that

$$\alpha(x_v - 1)(x_u - 1)\beta$$

can be expressed likewise, and this verifies our claim that in proving the theorem we are free to interchange the factors of π. □

Theorem 3.6. *The set $\{\eta \in \mathcal{B} : w(\eta) \geq i\}$ forms a basis for E_i as a $\mathbb{K}$-vector space. We call this the* ***Jennings basis*** *of E_i.*

Proof. Since the ηs are linearly independent, and because $w(\eta) \geq i$ implies $\eta \in E_i$, it will suffice to show that the set spans E_i. We shall do this by way of reversed induction on i.

According to Theorem 3.3, there is a d such that $E_d \neq \{0\} = E_{d+1}$. By Theorem 3.5, the statement is true for $i = d$. So, let $i \leq d$ and assume that every element in E_i can be expressed as a $\mathbb{K}$-linear sum of ηs with $w(\eta) \geq i$. According to Theorem 3.5, each element of E_{i-1} can be expressed as a $\mathbb{K}$-linear sum of ηs with weight $i-1$, modulo an element in E_i. Consequently, each element of E_{i-1} is expressable as a $\mathbb{K}$-linear sum of ηs with weight greater than or equal to $i-1$, and this concludes our proof. □

In Chapter 5, the following Hilbert type polynomial will prove to be the very key needed for unlocking the yet to be defined $\mathcal{M}$-series potential as a weapon for attacking modular isomorphism problems. The result is based upon a standard technique in combinatorics; the idea being to let polynomials do all the counting *for us*. In these types of arguments, making use of a so-called *generating function*, focus is on the exponents; the indeterminate, in this case y, is irrelevant.

Observe that since 1-stable N_p-series induce filtrations that stabilize at $\{0\}$, the sum on the left side is just a plain polynomial.

Theorem 3.7 (The Jennings formula). *Set $E_0 = \mathbb{K}[G]$. If $|G_s/G_{s+1}| = p^{e_s}$ and $G_d \neq G_{d+1} = \{1\}$, then*

$$\sum_{i=0}(\dim_{\mathbb{K}} E_i/E_{i+1})y^i = \Big(\frac{y^p-1}{y-1}\Big)^{e_1}\Big(\frac{y^{2p}-1}{y^2-1}\Big)^{e_2}\cdots\Big(\frac{y^{dp}-1}{y^d-1}\Big)^{e_d}.$$

That is, the coefficient of y^i in the product on the right is equal to the dimension of E_i/E_{i+1} as a $\mathbb{K}$-vector space.

Proof. The coefficient of y^i in the product

$$\big(1+y^{\nu(x_1)}+y^{2\nu(x_1)}+\cdots+y^{(p-1)\nu(x_1)}\big)\big(1+y^{\nu(x_2)}+y^{2\nu(x_2)}+\cdots+y^{(p-1)\nu(x_2)}\big)\cdots$$

$$\cdots\big(1+y^{\nu(x_n)}+y^{2\nu(x_n)}+\cdots+y^{(p-1)\nu(x_n)}\big)$$

is equal to the number of ways to pick $a_1, a_2, \ldots, a_n$ such that $0 \leq a_j \leq p-1$ and

$$a_1\nu(x_1)+a_2\nu(x_2)+\cdots+a_n\nu(x_n) = i.$$

According to Theorem 3.5, this is equal to $\dim_{\mathbb{K}} E_i/E_{i+1}$.

As the number of representatives with height s is equal to e_s, we obtain

$$\begin{aligned}
&\sum_{i=0}(\dim_{\mathbb{K}} E_i/E_{i+1})y^i \\
&\quad= \big(1+y^{\nu(x_1)}+y^{2\nu(x_1)}+\cdots+y^{(p-1)\nu(x_1)}\big)\big(1+y^{\nu(x_2)}+y^{2\nu(x_2)}+\cdots+y^{(p-1)\nu(x_2)}\big)\cdots \\
&\qquad\cdots\big(1+y^{\nu(x_n)}+y^{2\nu(x_n)}+\cdots+y^{(p-1)\nu(x_n)}\big) \\
&\quad= (1+y+y^2+\cdots+y^{(p-1)})^{e_1}(1+y^2+y^4+\cdots+y^{2(p-1)})^{e_2}\cdots \\
&\qquad\cdots(1+y^d+y^{d2}+\cdots+y^{d(p-1)})^{e_d} \\
&\quad= \Big(\frac{y^p-1}{y-1}\Big)^{e_1}\Big(\frac{y^{2p}-1}{y^2-1}\Big)^{e_2}\cdots\Big(\frac{y^{dp}-1}{y^d-1}\Big)^{e_d}.
\end{aligned}$$

□

Note that the application of this result in Chapter 5 will be somewhat unconventional: normally, when using generating functions to count something, one multiplies suitable polynomials (or formal power series) on the "right" side, in order to read off the answer from the coefficients of the resulting polynomial (formal power series) on the "left". We, on the other hand, shall be familiar with the coefficients on the "left" side, and demonstrate a way to obtain the numbers d and $e_i = \log_p |G_i/G_{i+1}|$ for $1 \leq i \leq d$.

3.3 A unique minimal N_p-series

Let $\mathcal{S}$ be the set consisting of all non-finite[1] N_p-series of G. The relation

$$\{G_i\} \leq \{H_i\} \text{ if and only if } G_i \leqslant H_i \text{ for all } i \geq 1$$

induces a partial order on $\mathcal{S}$.

We write $\{G_i\} = \{H_i\}$ if both $\{G_i\} \leq \{H_i\}$ and $\{H_i\} \leq \{G_i\}$, such that if $\{G_i\} = \{H_i\}$ then these series are equal *as series*, and not merely as sets of subgroups.

In accordance with standard terminology we say that the N_p-series $\{G_i\} \in \mathcal{S}$ is **minimal** if whenever $\{H_i\} \in \mathcal{S}$ and $\{H_i\} \leq \{G_i\}$, then $\{G_i\} = \{H_i\}$.

The main result of this section is that the series of dimension subgroups is *the* unique minimal element of $\mathcal{S}$.

Lemma 3.8. *Let $\{E_i\}$ be the filtration induced by a 1-stable N_p-series $\{G_i\}$, and let $g \in G$. Then $g \in G_i$ if and only if $g - 1 \in E_i$.*

[1] Cf. Section 2.2.

Proof. If $g \in G_i$, then $g-1 \in E_i$ by the definition of E_i. On the other hand, if $g \notin G_i$ then we know both that $\nu(g) < i$, and that $g \neq 1$. Let $\{H_i\}$ be a chief series refinement of $\{G_i\}$. Since $g \neq 1$ we have $g \in H_r \setminus H_{r+1}$ for some r. In choosing representatives for a Jennings basis, we are of course free to choose $x_r = g$, such that $g - 1 = \eta'(0, ..., 0, 1, 0, ..., 0)$, where the 1 occupies the "rth place".

According to Theorem 3.6 the ηs with $w(\eta) \geq i$ form a basis for E_i; since $w(\eta') = v(g) < i$ and because the ηs are linearly independent, we have $\eta' = g - 1 \notin E_i$. □

Theorem 3.9. *The series $\{\mathcal{D}_i\}$ of dimension subgroups is the unique minimal element of $\mathcal{S}$.*

Proof. The series is minimal. For assume $\{G_i\} \in \mathcal{S}$ and $\{G_i\} \leq \{\mathcal{D}_i\}$. Then $\{G_i\}$ is 1-stable, and we let $\{E_i\}$ denote its induced filtration. Let $g \in \mathcal{D}_i$. Then $g - 1 \in \Delta^i \subseteq E_i$, and according to Lemma 3.8 we have $g \in G_i$.

To prove uniqueness, we let $\{H_i\}$ be a minimal element of $\mathcal{S}$. Then

$$\{H_i \cap \mathcal{D}_i\} \leq \{\mathcal{D}_i\}$$

is also an N_p-series. From minimality of $\{\mathcal{D}_i\}$, we have

$$\{\mathcal{D}_i\} = \{H_i \cap \mathcal{D}_i\}$$

and, consequently,

$$\{\mathcal{D}_i\} \leq \{H_i\}.$$

As $\{H_i\}$ is minimal, this implies

$$\{H_i\} = \{\mathcal{D}_i\}.$$

□

Proposition 3.10. *Let $\{G_i\}$ be a 1-stable N_p-series and let $\{E_i\}$ be its induced filtration. If $\{H_i\}$ is the N_p-series derived from $\{E_i\}$, then $\{G_i\} = \{H_i\}$.*

Proof. If $g \in G_i$ then $g - 1 \in E_i$ and $g \in H_i$. Conversely, if $h \in H_i$, then $h - 1 \in E_i$ and by Lemma 3.8 we have $h \in G_i$. □

Similarly, if $\{G_i\}$ is the N_p-series derived from a filtration $\{E_i\}$, and if $\{F_i\}$ is the filtration induced by $\{G_i\}$, we may ask whether it is true that $E_i = F_i$ for all $i \geq 1$.

I am unaware if any of the two inclusions hold in general. The following theorem, however, shows that they both hold in the particular case when $\{G_i\}$ is the series of dimension subgroups.

Theorem 3.11. *The filtration induced by* $\{\mathcal{D}_i\}$ *is* $\{\Delta^i\}$.

Proof. Let $\{E_i\}$ be the filtration induced by $\{\mathcal{D}_i\}$. As we have already seen in the proof of Theorem 3.9, $\Delta^i = (E_1)^i \subseteq E_i$.

In order to show the opposite inclusion, we let

$$\pi = (g_1 - 1)(g_2 - 1) \cdots (g_k - 1)$$

be one of the generators for E_i, such that $w(\pi) \geq i$. As $g_j \in \mathcal{D}_{\nu(g_j)}$ we have $g_j - 1 \in \Delta^{\nu(g_j)}$, and therefore

$$\pi \in \Delta^{\nu(g_1)+\nu(g_2)+\cdots+\nu(g_k)} = \Delta^{w(\pi)} \subseteq \Delta^i.$$

Since π was an arbitrary generator, we conclude that $E_i \subseteq \Delta^i$. □

Chapter 4

The $\mathcal{M}$-series

Througout this chapter, let G be a group and let p be a fixed prime.

For $q \in \mathbb{Q}$ let $\lceil q \rceil$ denote the smallest integer greater than or equal to q.[1]

Definition. *For a group H, let $H^{(n)} = \langle h^n : h \in H \rangle$, the subgroup generated by all nth powers of elements of H.*

In [15], Jennings attributes the following definition to his Ph.D. supervisor Richard Brauer.

Definition. *We define the $\mathcal{M}$-**series** with respect to the prime p recursively by letting $\mathcal{M}_{1,p}(G) = G$, and*

$$\mathcal{M}_{i,p}(G) = [\mathcal{M}_{i-1,p}(G), G]\big(\mathcal{M}_{\lceil i/p \rceil,p}(G)^{(p)}\big) \text{ for } i > 1.$$

As long as either the prime p or *both* G *and* p is clear from the context, we shall write respectively $\mathcal{M}_i(G)$ or $\mathcal{M}_i$ in place of $\mathcal{M}_{i,p}(G)$.

Note that if H is a finite p-group, then

$$\mathcal{M}_2(H) = [H, H]H^{(p)} = \Phi(H).^2$$

After having established certain formalities – that $\mathcal{M}_i$ is in fact a subgroup, that $\mathcal{M}_i$ is characteristic in G, and that the sequence $\{\mathcal{M}_i\}$ is descending – we next investigate the case when G is abelian. This is done in Section 4.2, and much of the material found in that section is, to the best of my knowledge, new. Finally, we attempt a direct proof that the $\mathcal{M}$-series is an N-series. Although the attempt is ultimately unsuccessful, a certain progress *is* made.

The lemmas of this chapter are typically a little too specialized to be found in standard treatises on group theory, while too elementary to be included in articles. We will therefore, in general, offer them *with proofs*.

[1] This is commonly known as the *ceiling function*.

[2] See Appendix B.

Lemma 4.1. *If H and K are subgroups of G with either H or K normal, then HK is a subgroup of G.*

Proof. Standard result. See [31, Lemma 2.25 on p. 36]. □

Lemma 4.2. *$[H, G]$ is normal in G for every subgroup H.*

Proof. It suffices to show that $k^{-1}[h, g]k \in [H, G]$ for each generator $[h, g]$ of $[H, G]$ and each $k \in G$, and this is seen to be true from the equation

$$k^{-1}[h, g]k = [h, k]^{-1}[h, gk].$$

□

Proposition 4.3. *For each $i \geq 1$, $\mathcal{M}_i$ is a subgroup of G.*

Proof. By strong induction on i, the case $i = 1$ being trivially true.

Assume $\mathcal{M}_j$ is a subgroup of G for each $1 \leq j < i$. As $\lceil i/p \rceil < i$, both $[\mathcal{M}_{i-1}, G]$ and $\mathcal{M}^{(p)}_{\lceil i/p \rceil}$ are subgroups of G by the induction hypothesis. That $\mathcal{M}_i$ is a subgroup now follows immediately from lemmas 4.1 and 4.2. □

Proposition 4.4. *If $\{G_i\} \in \mathcal{S}$, the set of non-finite N_p-series, then $\mathcal{M}_i \leqslant G_i$ for all $i \geq 1$.*

Proof. By strong induction on i, the case $i = 1$ being $\mathcal{M}_1 = G = G_1$.

Let $i > 1$ and assume $\mathcal{M}_j \leqslant G_j$ for each $1 \leq j < i$. Then

$$[\mathcal{M}_{i-1}, G] \leqslant [G_{i-1}, G] \leqslant G_i,$$

and likewise,

$$\mathcal{M}^{(p)}_{\lceil i/p \rceil} \leqslant G^{(p)}_{\lceil i/p \rceil} \leqslant G_{p\lceil i/p \rceil} \leqslant G_i,$$

the last inclusion because $i \leq p\lceil i/p \rceil$. We conclude that

$$\mathcal{M}_i = [\mathcal{M}_{i-1}, G]\mathcal{M}^{(p)}_{\lceil i/p \rceil} \leqslant G_i.$$ □

4.1 A characteristic subgroup

Definition. *We say that a subgroup H of G is **characteristic**, and write H* char *G, if $\vartheta(H) = H$ for every automorphism ϑ of G.*

Since conjugation $h \mapsto g^{-1}hg$ is an automorphism of G for each $g \in G$, it is immediate that any characteristic subgroup is normal.

In this section, we show that each $\mathcal{M}_i$ is characteristic in G; a well-known fact already mentioned by Jennings in [15]. In light of the coming result that the $\mathcal{M}$-series is in fact equal to the series of dimension subgroups, this *also* serves to show that the dimension subgroups form a series of characteristic subgroups.

Note that in establishing whether a subgroup H is characteristic in G we may actually restrict our efforts to showing that $\vartheta(H) \leqslant H$ for every automorphism ϑ of G; because then $\vartheta^{-1}(H) \leqslant H$, and, consequently, $H = \vartheta(\vartheta^{-1}(H)) \leqslant \vartheta(H)$ as well.

Lemma 4.5. *Let H be a subgroup of G. If for every automorphism ϑ of G it is true that $\vartheta(\alpha) \in H$ for every generator α of H, then H char G.*

Proof. Let $h = \alpha_1\alpha_2\cdots\alpha_k \in H$, and let ϑ be an automorphism of G. Then $\vartheta(h) = \vartheta(\alpha_1)\vartheta(\alpha_2)\cdots\vartheta(\alpha_k) \in H$ and, due to the remarks preceding this lemma, we are done. □

Lemma 4.6. *If H, K char G, then HK char G.*

Proof. Clear. □

Lemma 4.7. *If H char G, then $H^{(n)}$ char G.*

Proof. Clear. □

Proposition 4.8. *For every $i \geq 1$, $\mathcal{M}_i$ is characteristic in G.*

Proof. The statement is clearly true for $i = 1$, since $\mathcal{M}_1 = G$. We proceed by way of strong induction on i. So, assume $\mathcal{M}_j$ char G for all $1 \leq j < i$, and consider $[\mathcal{M}_{i-1}, G]\mathcal{M}^{(p)}_{\lceil i/p \rceil}$. In light of Lemma 4.6, the subgroup $\mathcal{M}_i = [\mathcal{M}_{i-1}, G]\mathcal{M}^{(p)}_{\lceil i/p \rceil}$ is characteristic in G if each of $[\mathcal{M}_{i-1}, G]$ and $\mathcal{M}^{(p)}_{\lceil i/p \rceil}$ is characteristic in G.

Now, let ϑ be an automorphism of G. Then

$$\vartheta\big([\mathcal{M}_{i-1}, G]\big) = [\vartheta(\mathcal{M}_{i-1}), \vartheta(G)] = [\vartheta(\mathcal{M}_{i-1}), G],$$

which is equal to $[\mathcal{M}_{i-1}, G]$ by the induction hypothesis. Also, as $\lceil i/p \rceil < i$, the induction hypothesis and Lemma 4.7 together imply $\mathcal{M}^{(p)}_{\lceil i/p \rceil}$ char G, and this concludes our proof. □

Proposition 4.9. *The sequence $\{\mathcal{M}_i\}$ is descending.*

Proof. We first observe that $\mathcal{M}_2 \leqslant \mathcal{M}_1 = G$, since each $\mathcal{M}_i$ is a subgroup. Now let $i > 1$. Since $\mathcal{M}_{i-1}$ is normal in G by Proposition 4.8, we have

$$[\mathcal{M}_{i-1}, G] \leqslant \mathcal{M}_{i-1}.$$

Assume $\mathcal{M}_j \leqslant \mathcal{M}_{j-1}$ for all $1 < j < i$. Either $\lceil i/p \rceil = \lceil (i-1)/p \rceil$ and

$$\mathcal{M}^{(p)}_{\lceil i/p \rceil} = \mathcal{M}^{(p)}_{\lceil (i-1)/p \rceil} \leqslant \mathcal{M}_{i-1}$$

is trivially true; or $\lceil (i-1)/p \rceil = \lceil i/p \rceil - 1$, in which case

$$\mathcal{M}_{\lceil i/p \rceil} \leqslant \mathcal{M}_{\lceil (i-1)/p \rceil}$$

by the induction hypothesis, and

$$\mathcal{M}^{(p)}_{\lceil i/p \rceil} \leqslant \mathcal{M}^{(p)}_{\lceil (i-1)/p \rceil} \leqslant \mathcal{M}_{i-1}.$$

As both $[\mathcal{M}_{i-1}, G] \leqslant \mathcal{M}_{i-1}$ and $\mathcal{M}^{(p)}_{\lceil i/p \rceil} \leqslant \mathcal{M}_{i-1}$, we conclude that

$$\mathcal{M}_i \leqslant \mathcal{M}_{i-1}.$$

□

Having now established that the $\mathcal{M}$-series *is* in fact a series (cf. Section 2.2), we note that there is nothing a priori to suggest that it is in general 1-stable; to the contrary, it will become apparent at the beginning of Section 5 that this fails to be the case whenever G is not nilpotent.

4.2 When G is abelian

While trying to prove that the $\mathcal{M}$-series is an N-series, I decided to calculate some examples with finite abelian p-groups. For these groups, I discovered a pattern which resulted in a non-recursive expression for $\mathcal{M}_i$. Having searched quite thoroughly for the result elsewhere, I have only been able to find a passage in Passman's book [26, p. 670], saying that when G is abelian then *"clearly,* $\mathcal{M}_i = G^{(p^{i-1})}$*"*. This is incorrect, the simplest counterexample being $p = 2$ and $G = C_8$ (the cyclic group of order 8), when

$$\mathcal{M}_4 \cong C_2 \ncong \{1\} \cong C_8^{(2^3)}.$$

The correct expression is given in Proposition 4.12.

That being said, it is obvious from [15] that *Jennings knew how the $\mathcal{M}$-series of a finite abelian p-group behaves*, and he correctly gives the length of such a series.

Passman uses the faulty expression for $\mathcal{M}_i$ to "prove" that finite abelian p-groups split over fields of characteristic p; we shall attempt a dissimilar – and I hope correct – proof of this in Chapter 5.[3]

Lemma 4.10. *If G is an abelian group, then $G^{(n)} = \{g^n : g \in G\}$. Also then, $(G^{(n)})^{(m)} = G^{(nm)}$.*

Proof. By definition, $G^{(n)}$ is the smallest subgroup of G containing $\{g^n : g \in G\}$. For the first part it therefore suffices to show that when G is abelian, then $\{g^n : g \in G\}$ is itself a subgroup – which is easily verified.

The second part of the lemma then follows immediately from the associativity and commutativity of G. □

It appears the following function has not been used before in connection to the $\mathcal{M}$-series (or the series of dimension subgroups). The function is very well suited both for theoretical purposes and to simplify calculations. We shall use it repeatedly throughout the rest of this thesis.

Definition. *For $n, m \in \mathbb{N}$, let $[n]_m = \min\{m^k : k \in \mathbb{N} \text{ and } n \leq m^k\}$.*

E.g. $[18]_3 = 3^3$.
The following property is crucial to the inductive step of several proofs to come.

Lemma 4.11. *For every $n, m \in \mathbb{N}$, we have $[n]_m = m\left[\lceil \frac{n}{m} \rceil\right]_m$.*

Proof. Suppose $[n]_m = m^j$, so that $n = m^j - r$. Write r as $km + l$, where $0 \leq l < m$. Then $\frac{n}{m} = m^{j-1} - (k + \frac{l}{m})$, and $\lceil \frac{n}{m} \rceil = m^{j-1} - k$. If $m^{j-1} - k > m^{j-2}$, then $\left[\lceil \frac{n}{m} \rceil\right]_m = [m^{j-1} - k]_m = m^{j-1}$. In that case, $m\left[\lceil \frac{n}{m} \rceil\right]_m = m^j = [n]_m$ and we are done. We shall therefore assume that the opposite holds, and demonstrate that this leads to a contradiction. So, assume $m^{j-1} - k \leq m^{j-2}$, or, equivalently, that $m^{j-1} - m^{j-2} \leq k$. Then

$$r = km + l \geq (m^{j-1} - m^{j-2})m + l = m^j - m^{j-1} + l.$$

This in turn implies

$$n = m^j - r \leq m^j - (m^j - m^{j-1} + l) = m^{j-1} - l$$

and $[n]_m = m^{j-1}$: a contradiction. □

Proposition 4.12. *Let G be an abelian group. Then*

$$\mathcal{M}_i = G^{([i]_p)}.$$

[3] As mentioned in the introduction, this was first proven by Deskins in [5].

Proof. The proof is by strong induction on i. By definition,

$$\mathcal{M}_1 = G = G^{(p^0)} = G^{([1]_p)}.$$

Now let $i \geq 2$, and assume that the hypothesis holds for all $1 \leq j < i$. Since G is abelian,

$$\mathcal{M}_i = [\mathcal{M}_{i-1}, G]\mathcal{M}_{\lceil i/p \rceil}^{(p)} = \mathcal{M}_{\lceil i/p \rceil}^{(p)}.$$

As $\lceil i/p \rceil < i$, the induction hypothesis then yields $\mathcal{M}_i = \left(G^{([\lceil i/p \rceil]_p)}\right)^{(p)}$, which is equal to $\mathcal{M}_i = G^{(p[\lceil i/p \rceil]_p)}$ by Lemma 4.10. Finally, using Lemma 4.11 we see that $\mathcal{M}_i = G^{(p[\lceil i/p \rceil]_p)} = G^{(p\frac{1}{p}[i]_p)} = G^{([i]_p)}$. □

Using the above proposition, we proceed to find the length of the $\mathcal{M}$-series of a finite abelian p-group.

Lemma 4.13. *Let $m, n_1, n_2, \ldots, n_r \in \mathbb{N}$. Then*

$$(C_{m^{n_1}} \times C_{m^{n_2}} \times \cdots \times C_{m^{n_r}})^{(m)} \cong C_{m^{n_1-1}} \times C_{m^{n_2-1}} \times \cdots \times C_{m^{n_r-1}}.$$

Proof. As

$$(C_{m^{n_1}} \times C_{m^{n_2}} \times \cdots \times C_{m^{n_r}})^{(m)} = C_{m^{n_1}}^{(m)} \times C_{m^{n_2}}^{(m)} \times \cdots \times C_{m^{n_r}}^{(m)},$$

it suffices to show that $C_{m^n}^{(m)} \cong C_{m^{n-1}}$.

Assume that $C_{m^n} = \langle c \rangle$. Then $C_{m^n}^{(m)} = \langle c^m \rangle$. This is a cyclic group of order m^{n-1}, and as such necessarily isomorphic to $C_{m^{n-1}}$. □

As already mentioned, the following result coincides with that given by Jennings in [15]. The proof, however, is of course slightly different as we here use Proposition 4.12.

Proposition 4.14. *Let*

$$G \cong C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_r}}$$

be a finite abelian p-group. If $n = \max\{n_1, n_2, \ldots, n_r\}$, then the length of $\{\mathcal{M}_i(G)\}$ is p^{n-1}.

Proof. From Proposition 4.12 and Lemma 4.13 we see that

$$\begin{aligned} \mathcal{M}_{p^{n-1}} &\cong (C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_r}})^{(p^{n-1})} \\ &\cong \underbrace{C_p \times C_p \times \cdots \times C_p}_{\text{number of } i\text{'s with } n_i = n} \ncong \{1\}, \end{aligned}$$

while

$$\mathcal{M}_{p^{n-1}+1} \cong (C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_r}})^{(p^n)} \cong \{1\}.$$ □

A simplified $\mathcal{M}$-series could also be expected in the case when G is "almost abelian". For the sake of example, we take a look at $G \cong C_n \rtimes C_2$ – whose "non-abelian part" stems only from C_2.[4]

Proposition 4.15. *For $n \geq 3$, let $D_{2n} = \langle a, b : a^n = b^2 = 1, ba = a^{-1}b\rangle$ be the group of symmetries of a regular n-gon. Then*

$$\mathcal{M}_{i,2}(D_{2n}) = \langle a^{[i]_2}\rangle, \text{ for all } i > 1.$$

Proof. In order to find $[D_{2n}, D_{2n}]$, let $x, y \in D_{2n}$. From the relation $ba = a^{-1}b$, we may assume $x = a^{r_1}b^{s_1}$ and $y = a^{r_2}b^{s_2}$, where $s_{1,2} \in \{0, 1\}$. Clearly, the commutator $[x, y]$ contains an even number of bs. Using the relation $ba = a^{-1}b$, these may be assembled at the right (or left) side of the product, where they cancel each other out because $b^2 = 1$. We are left with an even number (possibly negative) of copies of a, which implies $[D_{2n}, D_{2n}] \leqslant \langle a^2\rangle$. Since $a^{2j} = [b, a^j]$, we conclude that $[D_{2n}, D_{2n}] = \langle a^2\rangle$.

As $(a^r b)^2 = 1$ we have $D_{2n}^{(2)} = \langle a^2\rangle$ as well, and

$$\mathcal{M}_2 = [D_{2n}, D_{2n}]D_{2n}^{(2)} = \langle a^2\rangle\langle a^2\rangle = \langle a^2\rangle.$$

Since the $\mathcal{M}$-series is descending we conclude that for all $i \geq 2$ we have $\mathcal{M}_i = \langle a^{2k}\rangle$ for some k. Using this, and the fact that

$$[a^k, a^r b] = a^{-k}ba^{-r}a^k a^r b = a^{-2k},$$

we see that

$$[\mathcal{M}_i, D_{2n}] = \mathcal{M}_i^{(2)} \text{ for all } i \geq 1.$$

Consequently,

$$\mathcal{M}_i = \mathcal{M}_{i-1}^{(2)}\mathcal{M}_{\lceil i/2\rceil}^{(2)} = \mathcal{M}_{\lceil i/2\rceil}^{(2)} \text{ for all } i \geq 2,$$

the last equality because $i - 1 \geq \lceil i/2\rceil$.

We are now ready to prove by strong induction that

$$\mathcal{M}_i = \langle a^{[i]_2}\rangle \text{ for all } i \geq 2,$$

with the case $i = 2$ already verified. Let $i > 2$ and assume that $\mathcal{M}_j = \langle a^{[j]_2}\rangle$ for all $2 \leq j < i$. Then

$$\mathcal{M}_i = \mathcal{M}_{\lceil i/2\rceil}^{(2)} = \langle a^{[\lceil i/2\rceil]_2}\rangle^{(2)} = \langle a^{2[\lceil i/2\rceil]_2}\rangle = \langle a^{[i]_2}\rangle,$$

by Lemma 4.11. □

[4]For a definition of the semi-direct product, see e.g. [31].

4.3 Attempting a direct proof that the $\mathcal{M}$-series is an N_p-series

In this section we attempt a direct proof that the $\mathcal{M}$-series is an N_p-series; a fact which was proven already by Jennings in [15] for the case of a finite p-group. That the result holds in general, can easily be deduced from e.g. [26, Theorem 1.20].

The $\mathcal{M}$-series certainly looks tailor made to fit the definitions of an N_p-sequence. Naively, one would expect the factor $[\mathcal{M}_{i-1}, G]$ to take care of strong centrality[5], and that $\mathcal{M}^{(p)}_{\lceil i/p \rceil}$ makes sure the series is p-restricted. And indeed,

Proposition 4.16. *If $x \in \mathcal{M}_i$, then $x^p \in \mathcal{M}_{ip}$.*

Proof.
$$x^p \in \mathcal{M}_i^{(p)} = \mathcal{M}^{(p)}_{\lceil \frac{ip}{p} \rceil} \leqslant [\mathcal{M}_{ip-1}, G]\mathcal{M}^{(p)}_{\lceil \frac{ip}{p} \rceil} = \mathcal{M}_{ip}. \qquad \square$$

Establishing the strong centrality has proven considerably more tricky, and will apparently end up using quite a few lemmas; some of which are trivial, others, such as the Hall-Petrescu formula, distinctly not so.

After having received a helpful suggestion from Dr. Benjamin Klopsch some time in December, I actually believed to have a valid proof for the case when G is a p-group. It was not until proofreading on the 28th of May that I discovered a hole in the proof; one which I have not been able to mend.

Lemma 4.17. *Suppose $H, K, L, N \leqslant G$, with N normal. If $[H, L] \leqslant N$ and $[K, L] \leqslant N$, then $[HK, L] \leqslant N$.*

Proof. Let $hk \in HK$ and $l \in L$. Letting n_i denote elements of N, we see that

$$\begin{aligned}[hk, l] &= k^{-1}h^{-1}l^{-1}hkl = k^{-1}h^{-1}l^{-1}hll^{-1}kl = k^{-1}n_1l^{-1}kl \\ &= k^{-1}n_1kk^{-1}l^{-1}kl = k^{-1}n_1kn_2 \\ &= k^{-1}kn_3n_2 \in N,\end{aligned}$$

which shows that any generator of $[HK, L]$ is contained in N. $\square$

Lemma 4.18. *Let H, K and N be subgroups of G, with N normal. If $[\alpha, \beta] \in N$ for every generator α of H and β of K, then $[H, K] \leqslant N$.*

[5] Since the lower central series is strongly central. For a proof of this, see [14, Theorem 4.11].

Proof. A typical generator of $[H, K]$ is

$$[h, k] = \alpha_r^{-1}\alpha_{r-1}^{-1}\cdots\alpha_1^{-1}\beta_s^{-1}\beta_{s-1}^{-1}\cdots\beta_1^{-1}\alpha_1\alpha_2\cdots\alpha_r\beta_1\beta_2\cdots\beta_s$$

where α_i and β_j are generators of H and K, respectively.

We are free to interchange the order of any product $\alpha_i\beta_j$ modulo N, that is: $\alpha_i\beta_j = \beta_j\alpha_i n$ for some $n \in N$. Because N is normal in G, this n may be replaced by another element n' of N – placed at the end of the product $[h, k]$.

For example, we have

$$\begin{aligned}[h, k] &= \alpha_r^{-1}\cdots\alpha_1^{-1}\beta_s^{-1}\cdots\beta_1^{-1}\alpha_1\cdots\alpha_r\beta_1\cdots\beta_s \\ &= \alpha_r^{-1}\cdots\alpha_1^{-1}\beta_s^{-1}\cdots\beta_2^{-1}\alpha_1\beta_1^{-1}n\alpha_2\cdots\alpha_r\beta_1\cdots\beta_s \\ &= (\alpha_r^{-1}\cdots\alpha_1^{-1}\beta_s^{-1}\cdots\beta_2^{-1}\alpha_1\beta_1^{-1}\alpha_2\cdots\alpha_r\beta_1\cdots\beta_s)n'\end{aligned}$$

Starting with α_1, and moving each α_i to the left all the way through $\beta_s^{-1}\beta_{s-1}^{-1}\cdots\beta_1^{-1}$, multiplying with elements of N from the right as we go, we eventually end up with

$$[h, k] = (\alpha_r^{-1}\alpha_{r-1}^{-1}\cdots\alpha_1^{-1}\alpha_1\cdots\alpha_r\beta_s^{-1}\beta_{s-1}^{-1}\cdots\beta_1^{-1}\beta_1\cdots\beta_s)n$$

with $n \in N$. □

The next result is due to the English mathematician Philip Hall ([7]).

Theorem 4.19 (Three-subgroups lemma). *Let N be a normal subgroup of G, and let $X, Y, Z \leqslant G$ be arbitrary subgroups. If both $\big[[X, Y], Z\big] \leqslant N$ and $\big[[Y, Z], X\big] \leqslant N$, then $\big[[Z, X], Y\big] \leqslant N$.*

Proof. See [14, Corollary 4.10]. □

I am grateful to Dr. Donald Passman for his suggestion to look at cases (i) and (ii), in the attempted proof that follows, separately.

Proposition 4.20. *For all $m, n \in \mathbb{N}$, we have $[\mathcal{M}_m, \mathcal{M}_n] \leqslant \mathcal{M}_{m+n}$.*

Attempted proof: Our strategy shall be doing strong induction on n (for all m). If $n = 1$ and $m \in \mathbb{N}$, then

$$[\mathcal{M}_m, \mathcal{M}_1] = [\mathcal{M}_m, G] \leqslant [\mathcal{M}_m, G]\mathcal{M}^{(p)}_{\lceil\frac{m+1}{p}\rceil} = \mathcal{M}_{m+1}.$$

For the induction step, let $n \geq 2$, and assume that for each $1 \leq k < n$,

$$[\mathcal{M}_j, \mathcal{M}_k] \leqslant \mathcal{M}_{j+k} \text{ for every } j \in \mathbb{N}.$$

Let $m \in \mathbb{N}$. As $\mathcal{M}_n = [\mathcal{M}_{n-1}, G]\mathcal{M}^{(p)}_{\lceil n/p\rceil}$, it will according to Lemma 4.17 suffice to show

(i) that $\big[\mathcal{M}_m, [\mathcal{M}_{n-1}, G]\big] \leqslant \mathcal{M}_{m+n}$, and

(ii) that $[\mathcal{M}_m, \mathcal{M}^{(p)}_{\lceil n/p \rceil}] \leqslant \mathcal{M}_{m+n}$.

For (i), we shall demonstrate that each of $\big[[G, \mathcal{M}_m], \mathcal{M}_{n-1}\big]$ and $\big[[\mathcal{M}_m, \mathcal{M}_{n-1}], G\big]$ is contained in $\mathcal{M}_{m+n}$; invoking the three-subgroups lemma then, we obtain the desired result. Keeping the induction hypothesis in mind, we see that

$$\begin{aligned}\big[[G, \mathcal{M}_m], \mathcal{M}_{n-1}\big] &= \big[[\mathcal{M}_m, G], \mathcal{M}_{n-1}\big] \\ &\leqslant [\mathcal{M}_{m+1}, \mathcal{M}_{n-1}] \\ &\leqslant \mathcal{M}_{m+1+n-1} \\ &= \mathcal{M}_{m+n}.\end{aligned}$$

And likewise,

$$\begin{aligned}\big[[\mathcal{M}_m, \mathcal{M}_{n-1}], G\big] &\leqslant [\mathcal{M}_{m+n-1}, G] \\ &\leqslant \mathcal{M}_{m+n-1+1} \\ &= \mathcal{M}_{m+n}.\end{aligned}$$

Hence $\big[\mathcal{M}_m, [\mathcal{M}_{n-1}, G]\big] = \big[[\mathcal{M}_{n-1}, G], \mathcal{M}_m\big] \leqslant \mathcal{M}_{m+n}$.

I have been unable to establish (ii).

Since we shall only make use of Theorem 4.20 in the case when G is a p-group, we may try to prove case (ii) given that restriction.

Under the assumption that G is a p-group

So, assume G is actually a p-group. I would like to thank Benjamin Klopsch for drawing my attention to Lemma 4.21 (below).

In order to prove (ii) it will, in light of Lemma 4.18, suffice to show that generators of the two subgroups commute modulo $\mathcal{M}_{m+n}$. Now let x be a generator for $\mathcal{M}_m$, and let $y \in \mathcal{M}_{\lceil n/p \rceil}$. According to Lemma 4.21, we have

$$[x, y^p] = [x, y]^p \mod \gamma_2(N)^{(p)}\gamma_p(N), \text{ where } N = \langle y, [x, y]\rangle.$$

As $\lceil n/p \rceil < n$, the induction hypothesis gives $[x, y] \in \mathcal{M}_{m+\lceil n/p \rceil}$. By Proposition 4.16 then, we have $[x, y]^p \in \mathcal{M}_{pm+p\lceil n/p \rceil} \leqslant \mathcal{M}_{pm+n} \leqslant \mathcal{M}_{m+n}$.

I have been unable to verify that $\gamma_2(N)^{(p)}\gamma_p(N) \leqslant \mathcal{M}_{m+n}$, which would complete our proof for the case when G is a finite p-group.

Lemma 4.21. *Let G be a p-group and $x, y \in G$. Then*

$$[x, y^p] = [x, y]^p \mod \gamma_2(N)^{(p)}\gamma_p(N), \text{ where } N = \langle y, [x, y]\rangle.$$

Proof. A corollary to the more famous Hall-Petrescu formula. See [2, p. 382]. □

Chapter 5

Applications

Throughout this chapter, let $\mathbb{K}$ be a field of characteristic p.

If we had accomplished our goal in Section 4.3 of proving directly that the $\mathcal{M}$-series is an N-series, this would have provided a new proof that

Theorem 5.1. *If G is a finite p-group and $\{\mathcal{D}_i(G)\}$ is the series of dimension subgroups derived from $\Delta(\mathbb{K}[G])$, then*

$$\{\mathcal{M}_{i,p}(G)\} = \{\mathcal{D}_i(G)\} \text{ for all } i \geq 1.$$

For in that case the combined results of Chapter 4 would have shown that $\{\mathcal{M}_i\}$ is contained in $\mathcal{S}$, the set of non-finite N_p-series; and the result would follow since $\{\mathcal{M}_i\} \leq \{\mathcal{D}_i\}$ by Proposition 4.4, and because $\{\mathcal{D}_i\}$ is the unique minimal element of $\mathcal{S}$ according to Theorem 3.9.

For a valid proof of Theorem 5.1, we refer to Jennings's [15, Theorem 5.5]. Just like in Jennings's article, the following now turns into a simple corollary.

Corollary 5.2. *Let G be a finite p-group, then $\{\mathcal{M}_{i,p}(G)\}$ is an N_p-series.*

Proof. Immediate from Theorems 3.1 and 5.1. □

The result here given as theorem 5.1 is actually independent of the group G, and only depends upon the characteristic of $\mathbb{K}$ being equal to p. A proof that the result holds for arbitrary groups can be found in e.g. [27] or [26].

The also has consequences for Corollary 5.2: as can readily be seen from the proof of Theorem 3.1, the dimension subgroups form an N_p-series regardless of the group G. In light of the previous remark, the series $\{\mathcal{M}_{i,p}(G)\}$ is therefore always an N_p-series – independent of whether G is a finite p-group or not.[1] The only parts relevant to the MIP, however, are Theorem 5.1 and Corollary 5.2.

[1] One immediate consequence of the $\mathcal{M}$-series being strongly central is that $\gamma_i \leqslant \mathcal{M}_i$ for all $i \geq 1$, and it is clear that $\{\mathcal{M}_i(G)\}$ is not 1-stable whenever G is not nilpotent.

5.1 The link

As announced towards the end of Section 3.2, we will now use the Jennings formula to establish invariants applicable for splitting groups. The single result of this section forms a crucial link between the $\mathcal{M}$-series of a finite p-group and this same groups modular group ring.

Theorem 5.3. *Let G be a finite p-group. Then $\mathbb{K}[G]$ determines*

(i) the length of the $\mathcal{M}$-series.

(ii) the factor groups $\mathcal{M}_{i,p}(G)/\mathcal{M}_{j,p}(G)$ for all $1 \leq i \leq j \leq 2i$.

Part (i) is well-known, and part (ii) is certainly not new – as it is stated (without proof) in [33]. It is a curious fact however, that this is about the only place one will be able to find it; other articles that offer a summary of known invariants, such as [6][2], [1], or [3], only display the weaker result that $\mathcal{M}_i/\mathcal{M}_{i+1}$ and $\mathcal{M}_i/\mathcal{M}_{i+2}$ is determined.

A possible explanation is that this was all that was proven in [28] – the article invariably cited in the above listed summaries. The proof in [28] is distinctly different from the one provided below.

The idea of using the Jennings formula to obtain the order of $\mathcal{M}_i/\mathcal{M}_{i+1}$ can be found in Passman's book [26, p. 670]. He however refrains from drawing the stronger conclusion (ii), and I also feel that the proof in [26] is lacking in that the length d is assumed to have been found already, somehow. But without further ado:

Proof. Let d denote the length of $\{\mathcal{M}_i\}$, and for $1 \leq i \leq d$ let

$$e_i = \log_p |\mathcal{M}_i/\mathcal{M}_{i+1}|,$$

such that $p^{e_i} = |\mathcal{M}_i/\mathcal{M}_{i+1}|$. We demonstrate a way to obtain both d and the numbers e_i from knowing $\mathbb{K}[G]$ as a $\mathbb{K}$-algebra.

As $\Delta(\mathbb{K}[G]) = \mathcal{J}\mathbb{K}[G]$ we may form the sum $\sum_{i=0}(\dim_{\mathbb{K}} \Delta^i/\Delta^{i+1})y^i$, which according to Theorem 3.7 is equal to

$$\Big(\frac{y^p-1}{y-1}\Big)^{e_1}\Big(\frac{y^{2p}-1}{y^2-1}\Big)^{e_2}\cdots\Big(\frac{y^{dp}-1}{y^d-1}\Big)^{e_d}.$$

Letting ζ_j denote the primitive complex (jp)th root of unity, the above product may be factorized as

$$\prod_{j=1}^{d}\Big(\prod_{\substack{i=1\\ p\nmid i}}^{jp}(y-\zeta_j^i)\Big)^{e_j}. \tag{5.1}$$

[2]The most up-to-date summary is found in this preprint.

Let $f_0(y) = \sum_{i=0}(\dim_{\mathbb{K}} \Delta^i/\Delta^{i+1})y^i$. Starting with $s = 1$, for increasing s and $1 \leq i \leq sp$, find the multiplicity $m_{s,i}$ of ζ_s^i as a root of $f_{s-1}(y)$. Performing polynomial division, set

$$f_s(y) = f_{s-1}(y) : \prod_{i=1}^{sp}(y - \zeta_s^i)^{m_{s,i}}.$$

As the degree of $\sum_{i=0}(\dim_{\mathbb{K}} \Delta^i/\Delta^{i+1})y^i$ is finite, there is a least $N \in \mathbb{N}$ such that $f_N(y) = 1$. Considering (5.1) it is clear that $N = d$. This proves (i).

From (5.1) we see that e_d is equal to the multiplicity of ζ_d as a root of $f_0(y)$, and in general that e_j is equal to the multiplicity of ζ_j as a root of

$$f_0(y)\Big(\prod_{\substack{i=1\\ p\nmid i}}^{dp}(y - \zeta_d^i)\Big)^{-e_d}\Big(\prod_{\substack{1=i\\ p\nmid i}}^{(d-1)p}(y - \zeta_{d-1}^i)\Big)^{-e_{d-1}} \cdots \Big(\prod_{\substack{i=1\\ p\nmid i}}^{(j+1)p}(y - \zeta_{j+1}^i)\Big)^{-e_{(j+1)}}.$$

Having retrieved each e_i recursively, (ii) follows. For if $1 \leq i < j \leq 2i$, then from Proposition 2.8 we know that $\mathcal{M}_i/\mathcal{M}_j$ is elementary abelian and therefore determined up to isomorphism by its order

$$|\mathcal{M}_i/\mathcal{M}_j| = p^{e_i} \cdots p^{e_{j-1}}. \qquad \square$$

In addition, it was established by Ritter and Sehgal in [30] that the modular group ring of a finite p-group determines $\mathcal{M}_i/\mathcal{M}_{2i+1}$; an immediate consequence being that any such group whose $\mathcal{M}$-series has length two is determined.

5.2 Finite abelian p-groups split

In this section we offer a new proof that finite abelian p-groups are determined by their modular group ring. We achieve this using the non-recursive expression for $\mathcal{M}_i$ found in Section 4.2. Recall from the introduction that the order of a finite group is determined. This implies that when splitting a pair of finite groups, we may presume their orders to be equal.

As before, we let C_n denote the cyclic group of order n. Recall from Lemma 4.13 that

$$(C_{m^{n_1}} \times C_{m^{n_2}} \times \cdots \times C_{m^{n_r}})^{(m)} \cong C_{m^{n_1-1}} \times C_{m^{n_2-1}} \times \cdots \times C_{m^{n_r-1}}.$$

Theorem 5.4. *If G and H are finite abelian p-groups with $\mathbb{K}[G] \cong \mathbb{K}[H]$, then $G \cong H$.*

Proof. Assume $G \ncong H$. As just mentioned, we also assume that $|G| = |H|$. Since G and H are finite abelian p-groups, there are unique natural numbers n_i, m_j, such that

$$G \cong C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$$

and

$$H \cong C_{p^{m_1}} \times C_{p^{m_2}} \times \cdots \times C_{p^{m_l}}.$$

Let s be the smallest number such that G and H have an unequal number of factors isomorphic to C_{p^s}. Then

$$|\mathcal{M}_{p^{s-1}+1}(G)| = |G^{[p^{s-1}+1]_p}| = |G^{(p^s)}| \neq |H^{(p^s)}| = |H^{[p^{s-1}+1]_p}| = |\mathcal{M}_{p^{s-1}+1}(H)|,$$

while

$$|\mathcal{M}_{p^{s-1}}(G)| = |G^{[p^{s-1}]_p}| = |G^{(p^{s-1})}| = |H^{(p^{s-1})}| = |H^{[p^{s-1}]_p}| = |\mathcal{M}_{p^{s-1}}(H)|.$$

As an immediate consequence we have

$$\mathcal{M}_{p^{s-1}}(G)/\mathcal{M}_{p^{s-1}+1}(G) \ncong \mathcal{M}_{p^{s-1}}(H)/\mathcal{M}_{p^{s-1}+1}(H),$$

which according to part (ii) of Theorem 5.3 implies $\mathbb{K}[G] \ncong \mathbb{K}[H]$. □

5.3 Extraspecial groups split

Recall that $\mathcal{Z}(G)$ denotes the center of a group G. See Appendix B for a definition of the Frattini subgroup $\Phi(G)$.

Definition. *A finite p-group G is said to be* ***extraspecial***[3] *if $\Phi(G) = \mathcal{Z}(G) = [G, G]$ has order p.*

In this section we prove that when p is an odd prime, extraspecial (p-)groups split over fields of characteristic p.

Theorem 5.5. *Every extraspecial group has order p^{2n+1}, for some $n \geq 1$. Conversely, if $n \geq 1$ there are exactly two distinct (isomorphism classes of) extraspecial groups of order p^{2n+1}.*

Proof. This is just an extract from Lemma 2.2.9, Theorem 2.2.10 and Theorem 2.2.11 of [20]. □

The **exponent** of a finite group H is the least $n \in \mathbb{N}$ such that $h^n = 1$ for all $h \in H$.

[3] A finite p-group H with $\Phi(H) = \mathcal{Z}(H) = [H, H]$ is just special.

Lemma 5.6. *For every prime $p > 2$, one of the extraspecial groups of order p^{2n+1} has exponent p, while the other has exponent p^2.*

Proof. See [20, Theorem 2.2.10]. □

Proposition 5.7. *Let $p > 2$ be a prime. If G_0 and G_1 are the two non-isomorphic extraspecial groups of order p^{2n+1}, then*

$$\mathbb{K}[G_0] \ncong \mathbb{K}[G_1].$$

Proof. Let G denote either G_0 or G_1. The fact that $[G,G]G^{(p)} = \Phi(G)$ (Theorem B.2) implies both $\mathcal{M}_2(G) = [G,G] \cong C_p$, and $G^{(p)} \leqslant [G,G]$. Since the order of a subgroup divides the order of a group, we either have $G^{(p)} \cong \{1\}$ or $G^{(p)} \cong C_p$. We assume – without loss of generality – that G_0 has exponent p (and hence that G_1 has exponent p^2). Then $\mathcal{M}_3(G_1) = G_1^{(p)} \ncong \{1\}$ implies $\mathcal{M}_3(G_1) \cong C_p$. It is equally clear that $\mathcal{M}_3(G_0) = G_0^{(p)} \cong \{1\}$.

Since $[G,G] = \mathcal{Z}(G)$, we have $[\mathcal{M}_2(G), G] = \big[[G,G],G\big] = \{1\}$, such that

$$\mathcal{M}_3(G) = [\mathcal{M}_2(G), G]\mathcal{M}_{\lceil \frac{3}{p} \rceil}(G)^{(p)} = \mathcal{M}_{\lceil \frac{3}{p} \rceil}(G)^{(p)} = G^{(p)}.$$

We conclude that

$$\frac{\mathcal{M}_2(G_0)}{\mathcal{M}_3(G_0)} \cong C_p \ncong \{1\} \cong \frac{\mathcal{M}_2(G_1)}{\mathcal{M}_3(G_1)},$$

and G_0 and G_1 split over $\mathbb{K}$ according to part (ii) of Theorem 5.3. □

Note that this argument fails for $p = 2$, as lemma 5.6 does not hold. Since Q_8 and D_8 are the only nonabelian groups of order 8, they are extraspecial by Theorem 5.5. It is however easy to check that both these groups have exponent 4. In Section 5.4 we shall apply a different technique, and show that D_8 and Q_8 split over $\mathbb{F}_{2^n}$ for n odd.

Also note that for $\mathbb{K} = \mathbb{F}_p$, Theorem 5.7 is an immediate consequence of [33, Theorem 6.25], which says that a finite p-group G of nilpotency class 2 with $[G,G]$ elementary abelian splits over the field of p elements.

5.4 Kernel size technique

It is not too difficult to find non-isomorphic finite p-groups that have isomorphic quotients $\mathcal{M}_i/\mathcal{M}_{i+1}$ for all $i \geq 1$, in which case Theorem 5.3 fails to be a splitting tool.

In this section, we describe an alternative technique for splitting groups, a technique which was also provided by Jennings in [15], in the sense

that its effectiveness depends on the ability to explicitly calculate bases for $\Delta(\mathbb{K}[G])^i/\Delta(\mathbb{K}[G])^{i+1}$ from (the $\mathcal{M}$-series of) a group G. From these bases we obtain numerical invariants of $\mathbb{K}[G]$.

Let G be a finite p-group. Then for all $r, t \in \mathbb{N}$ the map

$$f_{G,t} : \Delta^r/\Delta^{r+1} \to \Delta^{rt}/\Delta^{rt+1}$$

defined by

$$f_{G,t}(x + \Delta^{r+1}) = x^t + \Delta^{rt+1}$$

is well defined. For if $x - y \in \Delta^{r+1}$ then $x^t = (y + z)^t$ for some $z \in \Delta^{r+1}$, and $(y + z)^t = y^t + \gamma$ where $\gamma \in \Delta^{(t-1)r+(r+1)} = \Delta^{rt+1}$.

As the augmentation ideal is equal to the Jacobson radical, the cardinality of the kernel of $f_{G,t}$ is determined by $\mathbb{K}[G]$ as a $\mathbb{K}$-algebra. In particular, when $\mathbb{K}$ is finite, such that $\mathbb{K}[G]$ is finite as well, the number of elements in the kernel of $f_{G,t}$ is determined.

Assume from now on that $\mathbb{K}$ *is* finite. The algorithm for splitting non-isomorphic finite p-groups G and H over $\mathbb{K}$, goes as follows: Computing the series $\{\mathcal{M}_i(G)\}$ and $\{\mathcal{M}_i(H)\}$ – with respect to the prime p – one obtains Jennings bases for $\Delta(\mathbb{K}[G])^i/\Delta(\mathbb{K}[G])^{i+1}$ and $\Delta(\mathbb{K}[H])^i/\Delta(\mathbb{K}[H])^{i+1}$, respectively. The next and potentially impossible step, is to use these bases to calculate the kernel sizes of $f_{G,t}$ and $f_{H,t}$. If these two numbers do not match, then G and H split.

Choosing $t = p$ suggests itself, and with $r = 1$ one may still hope for the computations to be manageable by hand.

It appears that the first one to successfully apply this technique was Passman, who used it in [24] to show that D_8 and Q_8 split over $\mathbb{F}_2$. We shall extend his result by showing that

Proposition 5.8. *The groups D_8 and Q_8 split over $\mathbb{F}_{2^n}$ for every odd number n.*

Proof. Let

$$D_8 = \langle a, b : a^4 = 1, b^2 = 1, ba = a^{-1}b \rangle,$$

and

$$Q_8 = \langle a, b : a^4 = 1, b^2 = a^2, ba = a^{-1}b \rangle.$$

From Example 4.15 we know that

$$\mathcal{M}_1(D_8) = D_8 > \mathcal{M}_2(D_8) = \langle a^2 \rangle > \mathcal{M}_3(D_8) = \langle a^4 \rangle = \{1\}. \tag{5.2}$$

By arguments identical to the ones in that example, we have

$$[Q_8, Q_8] = \langle a^2 \rangle \text{ and } [\mathcal{M}_2(Q_8), G] = \{1\},$$

such that

$$\mathcal{M}_1(Q_8) = Q_8 > \mathcal{M}_2(Q_8) = \langle a^2 \rangle > \mathcal{M}_3(Q_8) = \langle a^4 \rangle = \{1\}. \tag{5.3}$$

As

$$D_8/\langle a^2 \rangle \cong C_2 \times C_2 \cong Q_8/\langle a^2 \rangle,$$

it is clear from (5.2) and (5.3) that

$$\mathcal{M}_i(D_8)/\mathcal{M}_{i+1}(D_8) \cong \mathcal{M}_i(Q_8)/\mathcal{M}_{i+1}(Q_8) \text{ for all } i \geq 1,$$

and Theorem 5.3 can tell us nothing.

Let G denote either D_8 or Q_8, and consider

$$f_{G,2} : \Delta(\mathbb{F}_{2^n}[G])/\Delta(\mathbb{F}_{2^n}[G])^2 \to \Delta(\mathbb{F}_{2^n}[G])^2/\Delta(\mathbb{F}_{2^n}[G])^3.$$

We observe that a chief series refinement of $\{\mathcal{M}_i(G)\}$ (without repetitions) is

$$H_1 = G > H_2 = \langle a \rangle > H_3 = \langle a^2 \rangle > H_4 = \{1\},$$

with representatives $b \in G \setminus H_2$, $a \in H_2 \setminus H_3$, and $a^2 \in H_3 \setminus H_4$.

By Theorem 3.5, the set of all

$$(b-1)^{r_1}(a-1)^{r_2}(a^2-1)^{r_3}$$

with $r_j \in \{0, 1\}$ and

$$r_1\nu(b) + r_2\nu(a) + r_3\nu(a^2) = r_1 + r_2 + 2r_3 = i$$

forms a basis for Δ^i/Δ^{i+1}. Hence $\{(b-1), (a-1)\}$ is a basis for Δ/Δ^2 and $\{(a^2-1), (a-1)(b-1)\}$ is a basis for Δ^2/Δ^3.

Let $x = s_1(b-1) + s_2(a-1) + \Delta^2 \in \Delta/\Delta^2$, then

$$\begin{aligned} f_{G,2}(x) &= s_1^2(b-1)^2 + s_1s_2(b-1)(a-1) + s_1s_2(a-1)(b-1) + s_2^2(a-1)^2 + \Delta^3 \\ &= s_1^2(b^2-1) + s_1s_2\big((b-1)(a-1) + (a-1)(b-1)\big) + s_2^2(a^2-1) + \Delta^3. \end{aligned}$$

Since $1 = -1$ in $\mathbb{F}_{2^n}$, we have

$$\begin{aligned} (b-1)(a-1) + (a-1)(b-1) &= (b-1)(a-1) - (a-1)(b-1) \\ &= ba - ab = ab - ba = ba^3 - ba \\ &= (a^2-1) + ba^3 - ba - a^2 + 1 \\ &= (a^2-1) + (ba-1)(a^2-1) \\ &= (a^2-1) \bmod \Delta^3, \end{aligned}$$

as $w\big((ba-1)(a^2-1)\big) = 3$. Because b^2-1 is equal to 0 in $\mathbb{F}_{2^n}[D_8]$ and equal to a^2-1 in $\mathbb{F}_{2^n}[Q_8]$, we conclude that

$$f_{D_8,2}(x) = (s_2^2 + s_1 s_2)(a^2-1) + \Delta^3$$

and

$$f_{Q_8,2}(x) = (s_1^2 + s_2^2 + s_1 s_2)(a^2-1) + \Delta^3.$$

As a^2-1 is a basis element for Δ^2/Δ^3, x is in the kernel if and only if the coefficient is equal to 0. In other words, the number of elements in the kernel of $f_{D_8,2}$ is equal to the number of zeroes in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the polynomial

$$y^2 + xy \in \mathbb{F}_{2^n}[x,y],$$

and likewise, the number of elements in the kernel of $f_{Q_8,2}$ is equal to the number of zeroes of

$$x^2 + y^2 + xy.$$

Since $y^2 + xy = 0$ if and only if $y = 0$ or $y = -x$, and being careful not to count $(0,0)$ twice, we see that there are $2^{n+1}-1$ elements in the kernel of $f_{D_8,2}$.

We now focus our attention on the homogeneous polynomial x^2+y^2+xy. Let $\mathbb{P}^n_{\mathbb{F}}$ denote projective n-space[4] over the field $\mathbb{F}$. Observe that there is a 1-1 correspondence between the solutions in $\mathbb{P}^1_{\mathbb{F}_{2^n}}$ of $x^2+y^2+xy=0$ and solutions in $\mathbb{F}_{2^n}$ of x^2+x+1 ($\in \mathbb{F}_{2^n}[x]$), given by $(a,b) \mapsto a/b$.

If $\mathbb{F}_{2^n}$ contains an element α such that $\alpha^2+\alpha+1=0$, then

$$\mathbb{F}_{2^n} \supseteq \mathbb{F}_2(\alpha) \cong \mathbb{F}_2[x]/\langle x^2+x+1\rangle \cong \mathbb{F}_4.$$

In that case, as $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ and because

$$n = [\mathbb{F}_{2^n} : \mathbb{F}_2] = [\mathbb{F}_{2^n} : \mathbb{F}_4][\mathbb{F}_4 : \mathbb{F}_2],$$

we see that $2 \mid n$.

Hence, if $2 \nmid n$ the equation $x^2+y^2+xy=0$ has only the trivial solution $(0,0)$, $\ker(f_{Q_8,t}) = \{0\}$, and D_8 and Q_8 split over $\mathbb{F}_{2^n}$. □

Corollary 5.9. *The groups D_8 and Q_8 split over $\mathbb{F}_2$.*

We remark that the above corollary is also an immediate consequence of a result by Sandling from 1996 ([34]), which says that finite metacyclic[5]

[4] See any introductory book on algebraic geometry.

[5] A group G is said to be metacyclic if it has a normal cyclic subgroup N with G/N cyclic.

p-groups are determined by their modular group ring over $\mathbb{F}_p$. Both Q_8 and D_8 have a normal cyclic subgroup isomorphic to C_4, namely $\langle a \rangle$, such that their respective quotients are isomorphic to C_2.

We now return to the proof of Proposition 5.8, and look at the case when n is even. It is a well-known fact from the theory of finite fields that

Lemma 5.10. *If m divides n, then $\mathbb{F}_{p^m}$ is contained in $\mathbb{F}_{p^n}$.*

Proof. See [17, Theorem 5.5.5]. □

So if $2 \mid n$, then $\mathbb{F}_{2^2} \subseteq \mathbb{F}_{2^n}$. In that case, there is an $\alpha \in \mathbb{F}_{2^n}$ with $\alpha^2 + \alpha + 1 = 0$. Since α is then a root of $x^2 + x + 1$, there is a $\beta \in \mathbb{F}_{2^n}$ such that

$$x^2 + x + 1 = (x - \alpha)(x - \beta).$$

We note that $\beta \neq \alpha$, for otherwise

$$x^2 + x + 1 = (x - \alpha)^2 = x^2 - 2\alpha x + \alpha^2 = x^2 + \alpha^2,$$

which is impossible – as the polynomial on the left has a term x and the one on the right does not. Hence, the equation $x^2 + y^2 + xy$ has the two distinct solutions $(\alpha, 1)$ and $(\beta, 1)$ in $\mathbb{P}^1_{\mathbb{F}_{2^n}}$.

The element $(\alpha, 1)$ yields $2^n - 1$ distinct nonzero solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of $x^2 + y^2 + xy$; one solution $k(\alpha, 1)$ for each $k \in \mathbb{F}_{2^n} \setminus \{0\}$. Likewise, we obtain $2^n - 1$ distinct nonzero solutions from $(\beta, 1)$. Since $k(\alpha, 1) = k(\beta, 1)$ would imply $\alpha = \beta$, we see that there are $2^{n+1} - 2$ distinct nonzero solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Including the trivial solution $(0, 0)$, we conclude that the equation $x^2 + y^2 + xy$ has $2^{n+1} - 1$ solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ when $2 \mid n$.

This does *not* imply that the groups D_8 and Q_8 do not split over $\mathbb{F}_{2^n}$ for n even, it simply means that if they do, then in order to prove it we would have to apply a different strategy than the one used to prove Proposition 5.8.

5.5 Splitting a pair of groups of order p^6 (p an odd prime)

In this section we use Theorem 5.3 to split a pair of non-abelian p-groups of order p^6 (for p an odd prime) over fields of characteristic p. The groups are the ones named $\phi(42)_b$ and $\phi_2(51)$ in Rodney James's table [16]. We rename them, such that

$$G = \Phi_2(42)_b = \langle a, b, c : [b, a] = c = a^{p^3}, b^{p^2} = c^p = 1, [a, c] = [b, c] = 1 \rangle$$

and

$$H = \Phi_2(51) = \langle a, b, c : [b, a] = c = a^{p^4}, b^p = c^p = 1, [a, c] = [b, c] = 1 \rangle.$$

Neither of these presentations are minimal, as c may be excluded from each of the generating sets. Keeping c makes for simpler computations. We shall calculate each of the $\mathcal{M}$-series (with respect to the prime p), but first we observe certain properties shared by both groups.

Since $ba = abc$, and because c commutes with all elements, we have

$$\cdots b^r a^s \cdots = \cdots a^s b^r c^{rs} \cdots = \cdots a^s b^r \cdots c^{rs}.$$

We may therefore assume that each element in either G or H is of the form $a^i b^j c^k$.

As

$$\begin{aligned}
[a^i b^j c^k, a^{i'} b^{j'} c^{k'}] &= c^{-k} b^{-j} a^{-i} c^{-k'} b^{-j'} a^{-i'} a^i b^j c^k a^{i'} b^{j'} c^{k'} \\
&= (b^{-j} a^{-i} b^{-j'} a^{-i'} a^i b^j a^{i'} b^{j'}) c^{-k-k'+k+k'} \\
&= b^{-j} a^{-i} b^{-j'} a^{-i'} a^i b^j a^{i'} b^{j'} \\
&= (a^{-i-i'+i+i'} b^{-j-j'+j+j'}) c^{ji'-j'(-i'+i+i')-j'(-i-i'+i+i')} \\
&= c^{ji'-j'i}
\end{aligned}$$

we have $[G, G] = \langle c \rangle = [H, H]$.

Also in both groups, we have

$$(a^i b^j c^k)(a^{i'} b^{j'} c^{k'}) = a^{i+i'} b^{j+j'} c^{k+k'+i'j},$$

and we prove by induction that

$$(a^i b^j c^k)^n = (a^{ni} b^{nj} c^{nk+\binom{n}{2}ij}) \text{ for all } n \geq 2.$$

This is clearly true for $n = 2$, and if it holds for $n - 1 \geq 2$ then

$$\begin{aligned}
(a^i b^j c^k)^n &= \left(a^{(n-1)i} b^{(n-1)j} c^{(n-1)k+\binom{n-1}{2}ij}\right)(a^i b^j c^k) \\
&= a^{ni} b^{nj} c^{nk+(\binom{n-1}{2}+n-1)ij} \\
&= a^{ni} b^{nj} c^{nk+\binom{n}{2}ij},
\end{aligned}$$

as $\binom{n-1}{2} + n - 1 = \binom{n}{2}$.

We proceed now to calculate the $\mathcal{M}$-series of G, and begin by finding $G^{(p)}$. If $g = a^i b^j c^k \in G$, then

$$g^p = a^{pi} b^{pj} c^{pk+\binom{p}{2}ij} = a^{pi} b^{pj},$$

as $p \mid \binom{p}{2}$ and $c^p = 1$. Since

$$[a^p, b^p] = a^{-p}b^{-p}a^pb^p = a^{-p+p}b^{-p+p}c^{(-p)p} = c^{(-p)p} = 1,$$

and because the order of a is p^4, we therefore have

$$\begin{aligned} G^{(p)} \cong & \langle a^p, b^p : (a^p)^{p^3} = (b^p)^p = 1, [a^p, b^p] = 1 \rangle \\ \cong & C_{p^3} \times C_p. \end{aligned}$$

The relation $c = a^{p^3}$ implies $[G, G] \leqslant G^{(p)}$, and hence

$$\mathcal{M}_2(G) = [G, G]G^{(p)} = \langle c \rangle G^{(p)} = G^{(p)}.$$

Combining this with the equation

$$[a^{pi}b^{pj}, a^{i'}b^{j'}c^{k'}] = c^{(pj)i' - j'(ip)} = 1,$$

we see that

$$[\mathcal{M}_i(G), G] = \{1\}, \text{ for all } i \geq 2.$$

We are now ready to prove that

$$\mathcal{M}_i(G) \cong (C_{p^3} \times C_p)^{(\frac{[i]_p}{p})}, \text{ for all } i \geq 2.$$

Note that for $2 \leq i \leq p$ we have $\lceil i/p \rceil = 1$ and $[i]_p = p$, such that

$$\mathcal{M}_i(G) = G^{(p)} \cong C_{p^3} \times C_p = (C_{p^3} \times C_p)^{(\frac{[i]_p}{p})}.$$

Now let $i > p$ and observe that this implies $\lceil i/p \rceil \geq 2$. Assume that

$$\mathcal{M}_j(G) \cong (C_{p^3} \times C_p)^{(\frac{[j]_p}{p})} \text{ for all } 2 \leq j < i.$$

Then

$$\mathcal{M}_i(G) = \mathcal{M}_{\lceil \frac{i}{p} \rceil}(G)^{(p)} \cong \left(\left(C_{p^3} \times C_p \right)^{(\frac{[\lceil i/p \rceil]_p}{p})} \right)^{(p)} \cong (C_{p^3} \times C_p)^{([\lceil i/p \rceil]_p)},$$

which is equal to $(C_{p^3} \times C_p)^{(\frac{[i]_p}{p})}$ by Lemma 4.11.

Observe that the length of $\{\mathcal{M}_i(G)\}$ is equal to $p^3 + 1$, as this is the least integer r such that $\frac{[r]_p}{p} = p^3$.

For H, we have $(a^ib^jc^k)^p = a^{ip}b^{jp}c^{kp+\binom{p}{2}ij} = a^{ip}$; identical arguments as for G then show that

$$\mathcal{M}_i(H) \cong (C_{p^4})^{(\frac{[i]_p}{p})}, \text{ for all } i \geq 2.$$

This implies that the length of $\{\mathcal{M}_i(H)\}$ is $p^4 + 1$, and we conclude from Theorem 5.3(i) that G and H split.

Appendix A

The Jacobson radical

Let R be a ring with unity. In order to study R through its irreducible left R-modules, one would clearly wish for these modules to be capable of telling different elements of R apart. Imagine otherwise: that there are elements $x, y \in R$ such that for every irreducible left R-module V we have $xv = yv$ for all $v \in V$. Then one will not by looking at irreducible left modules be able to distinguish between x and y. As this would be the case if and only if

$$x, y \in \bigcap_{\substack{V \text{ irr. left} \\ R\text{-module}}} \operatorname{Ann}(V),$$

one defines[1]

Definition. *The (left)* ***Jacobson radical***

$$\mathcal{J}R_\ell = \{x \in R : xV = \{0\} \text{ for every irreducible left } R\text{-module } V\}.$$

This is readily seen to be a (two-sided) ideal of R.

We may of course define a *right* Jacobson radical as well, in terms of irreducible right R-modules. Fortunately, the two radicals coincide, enabling us to omit the adjectives left/right and speak simply of the **Jacobson radical** $\mathcal{J}R$.

The ring R is said to be **semisimple** if $\mathcal{J}R = \{0\}$. It is a classic result by Maschke that

Theorem (Mascke's theorem). *If G is a finite group and $\mathbb{K}$ is a field whose characteristic does not divide $|G|$ (e.g. if $\operatorname{char}(\mathbb{K}) = 0$), then $\mathbb{K}[G]$ is semisimple.*

[1] There are many equivalent definitions of the Jacobson radical.

Much research in group rings has been devoted to the so-called **semisimplicity problem** of finding necessary and sufficient conditions on the field $\mathbb{K}$ and group G for $\mathbb{K}[G]$ to be semisimple. The most famous conjecture is the following extension of Maschke's theorem:

Conjecture. *The group ring $\mathbb{K}[G]$ is semisimple for every field of characteristic 0.*

Appendix B

The Frattini subgroup

Let G be a group. A subgroup M of G is **maximal** if $M < G$ and if there is no subgroup H with $M < H < G$.

Definition. *The* ***Frattini subgroup*** *of G, denoted $\Phi(G)$, is defined as the intersection of all maximal subgroups of G. If the (necessarily infinite) group H fails to have a maximal subgroup, we define $\Phi(G) = G$.*

The Frattini subgroup has some remarkable properties. All results (with proofs) can be found in [31], as well.

Definition. *An element $x \in G$ is a* ***nongenerator*** *if whenever $Y \subseteq G$ and $G = \langle x, Y \rangle$, then $G = \langle Y \rangle$.*

Theorem B.1. *The Frattini subgroup is the set of all nongenerators.*

The following result is the important one to us. We therefore provide it *with proof.*

Theorem B.2. *If G is a finite p-group, then*

$$\Phi(G) = [G,G]G^{(p)} \ \big(\textit{which we recognize as } \mathcal{M}_{2,p}(G)\big).$$

Proof. Let M be a maximal subgroup of G. Since G is a finite p-group, it is nilpotent. From [31, Theorem 5.40] then, we have that M is normal in G, and that $G/M \cong C_p$. The fact that G/M is abelian, is equivalent to $[G,G] \subseteq M$. Since $g^p = 1$ for all $g \in G/M$, we have both $[G,G]$ and $G^{(p)}$ contained in M. Since M was an arbitrary maximal subgroup, we conclude that $[G,G]G^{(p)} \leqslant \Phi(G)$.

Now recall that $G/[G,G]G^{(p)} = \mathcal{M}_{1,p}(G)/\mathcal{M}_{2,p}(G)$ is elementary abelian. Elementary abelian groups have no nontrivial nongenerators, so

$$\Phi(G/[G,G]G^{(p)}) = \{[G,G]G^{(p)}\}. \tag{B.1}$$

Since $[G,G]G^{(p)} \leqslant \Phi(G)$, and since maximal subgroups of $G/[G,G]G^{(p)}$ correspond to maximal subgroups of G containing $[G,G]G^{(p)}$, it is easy to check that $\Phi(G)$ is the inverse image of $\Phi(G/[G,G]G^{(p)})$ under the natural map from G to $G/[G,G]G^{(p)}$. From (B) then, we have $\Phi(G) = [G,G]G^{(p)}$. $\square$

Corollary B.3. *$G/\Phi(G)$ is elementary abelian.*

A **minimal generating set** of G is a generating set X such that no proper subset of X is a generating set of G.

Theorem B.4 (Burnside Basis Theorem). *Let G be a finite p-group, and assume that $G/\Phi(G) \cong \underbrace{C_p \times C_p \times \cdots \times C_p}_{n \text{ factors}}$. Then every minimal generating set of G consists of n elements.*

Addendum:

I realized just yesterday, on the 29th of may, while proofreading Theorem 5.3, that the order of $\mathcal{M}_i$ is (rather obviously, I'm afraid) determined by $\mathbb{K}[G]$.

$$|\mathcal{M}_i| = p^{e_i} p^{e_{i+1}} \cdots p^{e_d}.$$

Having had this in mind earlier would, as can readily be seen, have made the proofs in sections 5.2, 5.3 and 5.5 each a couple of lines shorter.

Bibliography

[1] Czeslav Baginski, Alexander Konovalov. *The modular isomorphism problem for finite p-groups with a cyclic subgroup of index p^2*, arXiv:math/0607292v1 [math.RA], 2006.

[2] Yakov Berkovich. *Groups of prime power order. Volume 1*, Walter de Gruyter, Berlin, 2008.

[3] Frauke Bleher, Wolfgang Kimmerle, Klaus W. Roggenkamp, Martin Wursthorn. *Computational aspects of the isomorphism problem*, Algorithmic algebra and number theory, 313-329, Springer Berlin, 1999.

[4] Donald B. Coleman. *On the modular group ring of a p-group*, Proc. Amer. Math. Soc., **15**, 511-514, 1964.

[5] W. E. Deskins. *Finite abelian groups with isomorphic group algebras*, Duke Math. J., **23**, 35-40, 1956. Springer-Verlag, Berlin Heidelberg, 1993.

[6] Bettina Eick, Alexander Konovalov. *The modular isomorphism problem for the groups of order 512*, (preprint) Accepted for Proceedings of Groups St. Andrews 2009 (available August 2011).

[7] Philip Hall. *A contribution to the theory of groups of prime-power order*, Proc. Lond. Math. Soc., **36**, 29-95, 1934.

[8] Marshall Hall, jr. *The theory of groups*, The Macmillan Company, New York, 1959.

[9] I. N. Herstein. *Noncommutative rings*, George Banta Company, Menasha Wisconsin, 1968.

[10] Martin Hertweck. *A counterexample to the isomorphism problem for integral group rings*, The Annals of Mathematics, **154** (No.1), 115-138, 2001.

[11] G. Higman. *Units in group rings*, D. Phil. thesis, Oxford Univ., 1940.

[12] B. Huppert, N. Blackburn, 1982, *Finite Groups II*, Springer-Verlag, Berlin, 1940.

[13] Martin Hertweck, Marcos Soriano. *On the modular isomorphism problem: groups of order* 2^6, Contemporary Mathematics, **420**, 177-213, 2006.

[14] I. Martin Isaacs. *Finite group theory*, Graduate Studies in Mathematics, **92**, American Mathematical Society, Rhode Island, 2008.

[15] S. A. Jennings. *The structure of the group ring of a p-group over a modular field*, Transactions of the American Mathematical Society, **50** (No.1), 175-185, 1941.

[16] Rodney James. *The groups of order* p^6 *(p an odd prime)*, Mathematics of Computation, **34** (No.150), 613-637, 1980.

[17] Serge Lang. *Algebra, 3rd. edition*, Springer-Verlag Inc., New York, 1993.

[18] Y. A. Lam. *A first course in noncommutative rings*, Springer-Verlag, New York, Inc, 2001.

[19] Michel Lazard. *Sur les groupes nilpotents et les anneaux de Lie*, Annales scientifiques de l'É.N.S, **71**, 1954.

[20] C. R. Leedham-Green, S. McKay. *The structure of groups of prime power order*, Oxford University Press, Oxford, 2002.

[21] Gerald Losey. *On group algebras of p-groups*, Michigan Math. J., **7**, 237-240, 1960.

[22] Roman Mikhailov, Inder Bir Singh Passi. *Lower central and dimension series of groups*, Lecture Notes in Mathematics, **1952**, Springer-Verlag Berlin, 2009.

[23] Donald S. Passman. *Isomorphic groups and group rings*, Pacific J. Math., **15**, 561-583, 1965.

[24] Donald S. Passman. *The group algebras of groups of order* p^4 *over a modular field*, Michigan Math. J., **12**, 405-415, 1965.

[25] Donald S. Passman. *What is a group ring?*, Amer. Math. Monthly, **83** (No.3), 173-185, 1976.

[26] Donald S. Passman. *The algebraic structure of group rings*, Wiley-Interscience, New York, 1977.

[27] Inder Bir Singh Passi. *Group rings and their augmentation ideals*, Lecture Notes in Mathematics, **715**, Springer-Verlag Berlin, 1978.

[28] Inder Bir Singh Passi, Sudarshan K. Sehgal. *Isomorphism of modular groups algebras*, Math. Z., **129**, 65-73, 1972.

[29] J. Petrescu. *Sur les commutateurs*, Math. Z., **61**, 348-356, 1954.

[30] Jurgen Ritter, Sudarshan Sehgal. *Isomorphism of group rings*, Arch. Math. Basel, **40** (No. 1), 32-39, 1983.

[31] Joseph J. Rotman. *An introduction to the theory of groups*, Springer-Verlag Inc., New York, 1995.

[32] Mohammed A. M. Salim, Robert Sandling. *The modular group algebra problem for groups of order p^5*, J. Austral. Math. Soc. Ser. A, **61**, 229-237, 1996.

[33] Robert Sandling. *The isomorphism problem for group rings: a survey*, Lecture Notes in Mathematics, **1142**, 256-288, 1985.

[34] Robert Sandling. *The modular group algebra problem for metacyclic p-groups*, Proc. Amer. Math. Soc., **124** (No. 5), 1347-1350, 1996.